FortiClient EMS for Chromebooks - Administration Guide

VERSION 1.2.1

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

November 27, 2017

FortiClient EMS for Chromebooks 1.2.1 Administration Guide

04-121-436863-20171127

TABLE OF CONTENTS

Change Log

Date	Change Description
2017-07-06	Initial release.
2017-07-25	Upgrading Microsoft SQL Server Express to Microsoft SQL Server Standard or Enterprise on page 24 and Testing the SQL server upgrade on page 26 added.
2017-08-18	Added Extending license expiries on page 22.
2017-09-14	Added details to Adding the FortiClient Web Filter extension on page 28.
2017-11-27	Added details on safe search regarding Google search results and YouTube access. See Web Filter on page 54.

Introduction

FortiClient Enterprise Management Server for Chromebooks (FortiClient EMS for Chromebooks) is a security management solution that works with the FortiClient Web Filter extension to provide web filtering for Google Chromebook users.

FortiClient EMS for Chromebooks is designed to meet the needs of small to large enterprises that provide web filtering for Google Chromebook users. Benefits of deploying FortiClient EMS for Chromebooks include:

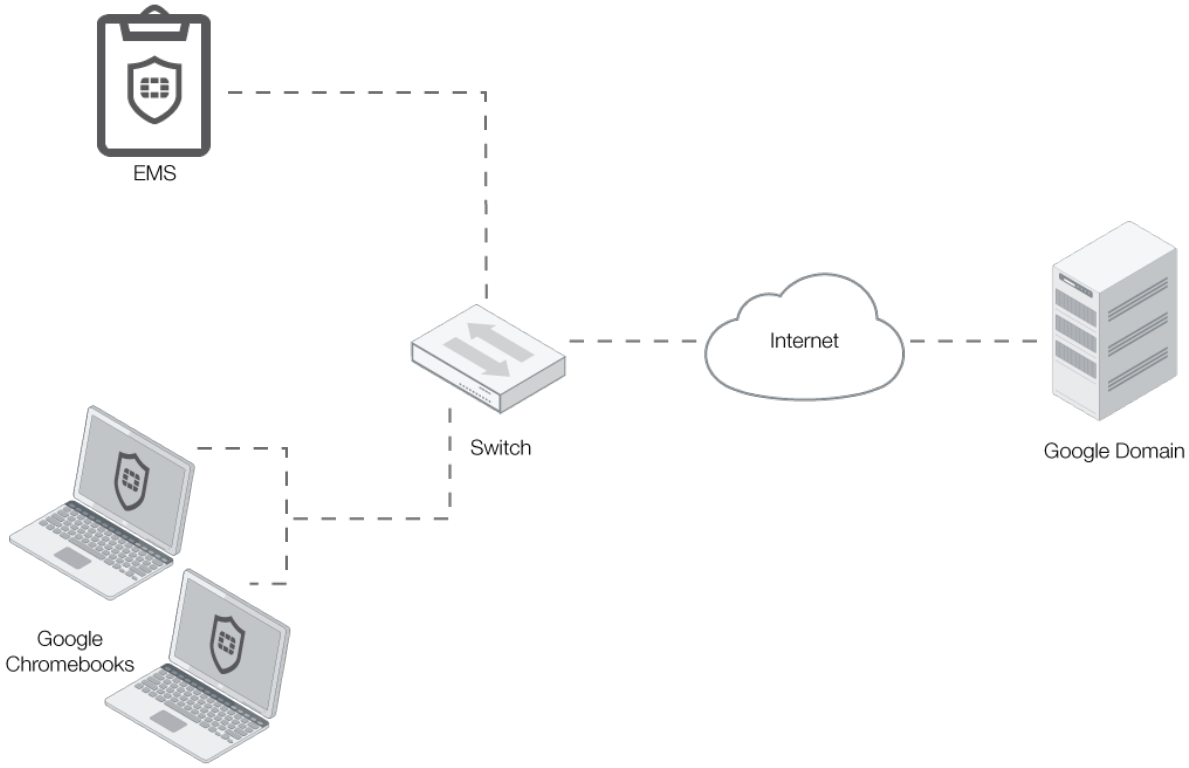
- Defining web filtering rules in a profile and remotely deploying the profile to the FortiClient Web Filter extension on Google Chromebook endpoints
- Updating profiles for Google Chromebook users regardless of access location
- Monitoring Google Chromebook endpoints

FortiClient EMS for Chromebooks components

FortiClient EMS for Chromebooks provides the infrastructure to install and manage the FortiClient Web Filter extension on Google Chromebook endpoints. FortiClient protects endpoint users by working with FortiClient EMS for Chromebooks to filter web content endpoint users view on Google Chromebooks.

The following table lists the FortiClient EMS for Chromebooks components.

Component	Description
FortiClient EMS for Chromebooks	Manages web filtering on Google Chromebook endpoints with the FortiClient Web Filter extension installed that connect to your Google domain. It includes the following software: • Console software that manages security profiles and Chromebook endpoints. • Server software that provides secure communication to and from Chromebook endpoints and the Google Admin console.
Database	Stores security profiles, events, and user information retrieved from the Google Admin console. The SQL database is installed as part of the FortiClient EMS for Chromebooks installation.
FortiClient Web Filter extension	Communicates with FortiClient EMS for Chromebooks and enforces web filtering on Google Chromebook endpoints.



FortiClient EMS for Chromebooks allows you to:

- Establish and enforce security profiles
- Manage security profiles from an integrated management console
- Obtain a consolidated view of multiple security profiles across all endpoints in your Google domain
- Monitor endpoints' web browsing activity

FortiClient EMS for Chromebooks and Fortinet Endpoint Security Management

FortiClient EMS for Chromebooks is part of the Fortinet Endpoint Security Management suite, which ensures comprehensive policy administration and enforcement for an enterprise network.

Documentation

You can access FortiClient EMS for Chromebooks documentation from the following link:
docs.fortinet.com/ems/admin-guides

The FortiClient EMS for Chromebooks documentation set includes the following:

- *FortiClient EMS for Chromebooks 1.2.1 Release Notes*

This document describes new features and enhancements in FortiClient EMS for Chromebooks for the release and lists any known issues and limitations. This document also defines supported platforms and minimum system requirements.

- *FortiClient EMS for Chromebooks 1.2.1 QuickStart Guide*

  This document describes how to install and begin working with the FortiClient EMS for Chromebooks system. It provides instructions on installation and deployment, and includes a high-level task flow for using the FortiClient EMS for Chromebooks system.

- *FortiClient EMS for Chromebooks 1.2.1 Administration Guide*

  This document describes how to set up FortiClient EMS for Chromebooks and use it to manage Chromebook endpoints. It includes information on how to configure multiple endpoints, configure and manage profiles for the endpoints, and view and monitor Chromebook endpoints.

What's New

The following is a list of new features and enhancements in FortiClient EMS for Chromebooks 1.2.

FortiClient EMS for Chromebooks 1.2.0

Pre-login banner

The pre-login banner can be used to display a message on the login page for FortiClient EMS for Chromebooks before the user logs in. Users must accept the banner message before they can log in. See Configuring the pre-login banner on page 64.

Separate license for EMS Chromebook support

Users can purchase a license applicable for FortiClient EMS and FortiClient EMS for Chromebooks. Alternatively, they can purchase licenses only applicable for FortiClient EMS for Chromebooks for a lower price.

FortiClient EMS for Chromebooks 1.2.1

FortiClient EMS for Chromebooks 1.2.1 does not contain new features or enhancements.

Get Started

This section provides an overview of how to perform the following tasks after you install and license FortiClient EMS for Chromebooks.

- Configuring FortiClient EMS for Chromebooks on page 11
- Configuring the Google Admin console on page 11
- Deploying profiles to Chromebooks on page 11

This section also includes a description of how FortiClient EMS for Chromebooks and FortiClient work with Google Chromebooks after setup is complete.

Configuring FortiClient EMS for Chromebooks

To configure FortiClient EMS for Chromebooks:

1. Start and log into FortiClient EMS for Chromebooks. See Starting FortiClient EMS for Chromebooks and logging in on page 20.
2. Add SSL certificates. See Adding SSL certificates to FortiClient EMS for Chromebooks on page 65.
3. Configure FortiClient EMS for Chromebooks settings. See Settings on page 62.
4. Configure user accounts and permissions. See User Management on page 58.

Configuring the Google Admin console

Following is an overview of how to configure the Google Admin console to prepare for adding the Google domain to FortiClient EMS for Chromebooks. The document assumes you have created the Google domain.

To configure the Google Admin console:

1. Add the FortiClient Web Filter extension. See Adding the FortiClient Web Filter extension on page 28.
2. Configure the FortiClient Web Filter extension. See Configuring the FortiClient Web Filter extension on page 29.
3. Add root certificates. See Adding root certificates on page 30.
4. Configure unique service account credentials. See Configuring unique service account credentials on page 38.
5. Disallow incognito mode. See Disallowing incognito mode on page 33.

Deploying profiles to Chromebooks

Following is an overview of how to add a Google domain, configure profiles, and push profiles to Google Chromebooks. After you add the extension in the Google Admin console, the extension is downloaded to the Google Chromebook when the Chromebook user logs into the Chromebook.

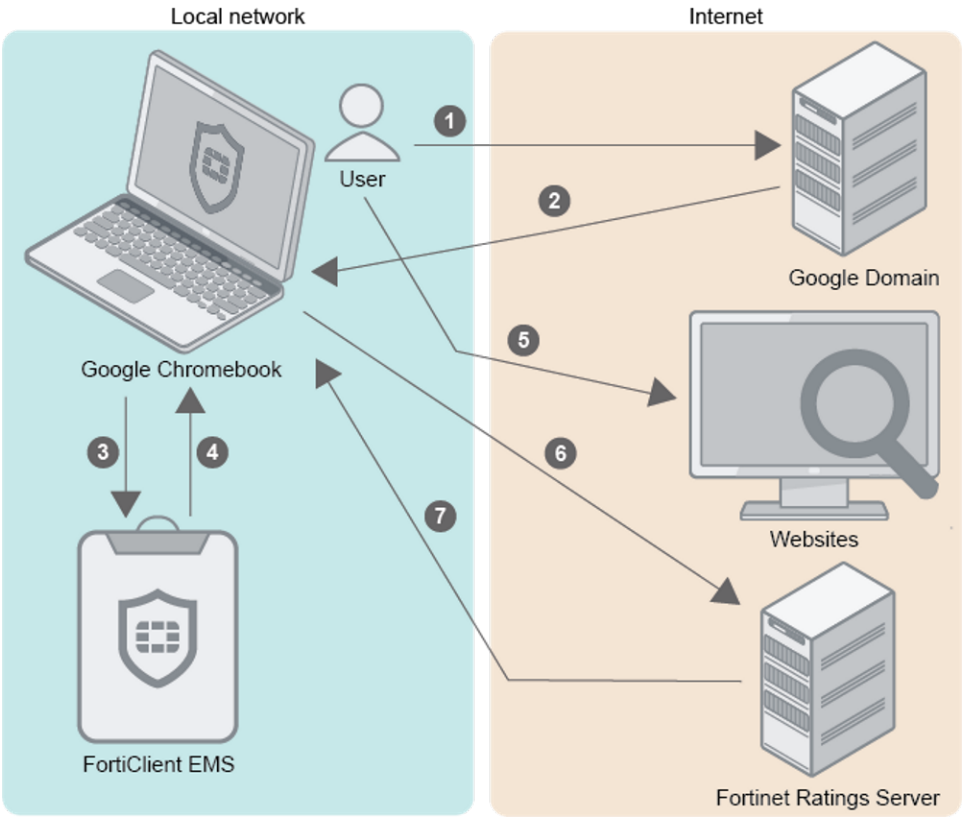
To deploy profiles to Chromebooks:

1. Add the Google domain. See Adding Google domains on page 47.
2. Define web filtering options in one or more profiles. See Configuring profiles on page 51.
   You can enable Safe Search in profiles.
3. Assign profiles to domains to deploy profiles to the FortiClient Web Filter extension on Chromebook endpoints. See Assigning profiles to Google Chromebooks on page 53.
4. Verify the FortiClient Web Filter extension. See Verifying the FortiClient Web Filter extension on page 35.
5. View Google domains and Google users. See Viewing domains on page 47.

How FortiClient EMS for Chromebooks and FortiClient work with Chromebooks

After you install and configure FortiClient EMS for Chromebooks, the Google Admin console, and the FortiClient Web Filter extension, the products work together to provide web filtering security for Google Chromebook users logged into the Google domain. Following is a summary of how the products work together after setup is complete:

1. A user logs into the Google Chromebook.
2. The Google Chromebook downloads the FortiClient Web Filter extension.
3. FortiClient connects to FortiClient EMS for Chromebooks.
4. FortiClient downloads a profile to the Google Chromebook. The profile contains web filtering settings from FortiClient EMS for Chromebooks.
5. The user browses the Internet on the Google Chromebook.
6. FortiClient sends the URL query to the Fortinet Ratings Server.
7. The Fortinet Ratings Server returns the category result to FortiClient. FortiClient compares the category result with the profile to determine whether to allow the Google Chromebook user to access the URL.


Local network
Internet
User
1
2
Google Domain
Google Chromebook
5
3
4
6
7
Websites
FortiClient EMS
Fortinet Ratings Server

Installation Preparation

This section helps you prepare to install FortiClient EMS for Chromebooks. Before installing FortiClient EMS for Chromebooks, be aware of the following information.

Before installing FortiClient EMS for Chromebooks, it is recommended you read the *FortiClient EMS for Chromebooks Release Notes* available on docs.fortinet.com to become familiar with relevant software components and other important information about the product.

Licenses

This section describes licensing options available for FortiClient EMS for Chromebooks. It provides information about the number of supported Google Chromebooks for each type of license to help determine which license best suits your needs.

FortiClient EMS for Chromebooks

FortiClient EMS for Chromebooks supports the following types of licenses:

- Free trial license
- Purchased license

Free trial license

When you install FortiClient EMS for Chromebooks, the free trial license is enabled by default. The free trial license supports ten Google Chromebook users. FortiClient EMS for Chromebooks consumes one license count per logged-in user. If the user logs out, the license seat times out (default timeout being 24 hours), and the license is released. At this point, another user can use this license seat.

Purchased license

Each purchased license allows management of one Google Chromebook user. You must purchase a minimum of 100 Google Chromebook users and can have this EMS license for a maximum three year term. You can specify the number of Google Chromebook users and the term duration at the time of purchase. FortiClient EMS for Chromebooks uses one license seat per logged-in user. If the user logs out, the license seat times out (default timeout being 24 hours), and the license is released. At this point, another user can use this license seat.

An email is sent when you are running out of licenses. Additionally, a log entry is entered when a client is refused connection due to unavailable licenses.

Component applications

Common services or applications do not require a license.

During the installation of common services required for FortiClient EMS for Chromebooks, you are not asked for license information.

Required services and ports

You must ensure required ports and services are enabled for use by FortiClient EMS for Chromebooks and its associated applications on your server. The required ports and services enable FortiClient EMS for Chromebooks to communicate with endpoints and servers running associated applications.

Communication	Service	Protocol	Port
Apache	HTTPS	TCP	443
SQL server			
FortiClient on Chrome OS • Connection to Profile Server.			8443 (default) You can customize this port.

Management capacity

FortiClient EMS for Chromebooks is intended for use by enterprises. It has the capacity to manage a large number of endpoints. The following are suggested host system hardware configurations for FortiClient EMS for Chromebooks. The suggested configurations depend on the number of endpoints being managed by FortiClient EMS for Chromebooks.

You need at least 200 GB of free disk space available.

Maximum number of managed endpoints	Number of virtual CPUs	Memory (RAM) (in GB)	Suggested keep alive interval
10000	2	8	default
20000	4	8	default
30000	4	8	120 seconds

Maximum number of managed endpoints	Number of virtual CPUs	Memory (RAM) (in GB)	Suggested keep alive interval
40000	4	8	120 seconds
50000	4	8	120 seconds
Suggested minimum system hardware for FortiClient EMS for Chromebooks:			
75000	8	16	120 seconds

For the purpose of this table, an Intel i5 processor with two cores and two threads per core is considered to have four virtual CPUs. An Intel i3 processor with two cores and one thread per core has two virtual CPUs.

Server readiness checklist for installation

Use the following checklist to prepare your server for installation.

Checklist	Readiness Factor
	Temporarily disable security applications. You must temporarily disable any antivirus software on the target server before you install FortiClient EMS for Chromebooks. Installation may be slow or disrupted while these programs are active. Note a server may be vulnerable to attack when you uninstall or disable security applications.
	It is recommended to sync the time to the Google server time.
	Confirm required services and ports are enabled and available for use by FortiClient EMS for Chromebooks.
	Ensure no conflict exists with port 443 for the Apache service to function properly.
	Ensure no conflict exists with port 8013 for the EMS service to function properly.

G Suite account

You need to sign up for your G Suite account before you can use the Google service and manage your Chromebook users.

The G Suite account is different from the free consumer account. The G Suite account is a paid account that gives access to a range of Google tools, services, and technology.

You can sign up for a G Suite account here: https://gsuite.google.com/signup/basic/welcome#0

In the sign up process, you must use your email address to verify your Google domain. This also proves you have ownership of the domain.

SSL certificates

FortiClient EMS for Chromebooks requires an SSL certificate signed by a Certificate Authority (CA) in pfx format. Use your CA to generate a certificate file in pfx format, and remember the configured password. For example, the certificate file name is *server.pfx* with password 111111.

The server where FortiClient EMS for Chromebooks is installed should have a fully qualified domain name (FQDN), such as ems.forticlient.com, and you must specify the FQDN in your SSL certificate.

If you're using a public SSL certificate, the FQDN can be included in *Common Name* or *Subject Alternative Name*. You must add the SSL certificate to FortiClient EMS for Chromebooks. See Adding SSL certificates to FortiClient EMS for Chromebooks on page 65. You do not need to add the root certificate to the Google Admin console.

If you're using a self-signed certificate (non-public SSL certificate), your certificate's *Subject Alternative Name* must include `DNS:<FQDN>`, for example, `DNS:ems.forticlient.com`. You must add the SSL certificate to FortiClient EMS for Chromebooks and the root certificate to the Google Admin console to allow the extension to trust FortiClient EMS for Chromebooks. See Adding root certificates on page 30.

Upgrading from an earlier FortiClient EMS for Chromebooks version

FortiClient EMS for Chromebooks 1.2.1 supports upgrading from FortiClient EMS for Chromebooks 1.0.3 and later 1.0 versions. To ensure a successful upgrade, it is recommended you perform the upgrade on a staging server before upgrading the production server. Follow the procedure below.

1. (Optional) Back up the database from the EMS 1.0.x production server.
2. Install EMS 1.0.x on a staging server.
3. (Optional) Import the EMS 1.0.x database from the production server.
4. Register FortiClient endpoints to the staging server.
5. Upgrade the staging server to EMS 1.2.1.
6. Monitor the staging server for two days.
7. Upgrade the production server to EMS 1.2.1.

Installation and Licensing

Before you install and license FortiClient EMS for Chromebooks on a server, ensure you have:

- Reviewed Licenses on page 14
- Met the requirements listed in Required services and ports on page 15
- Completed the Server readiness checklist for installation on page 16
- Logged into the server as the administrator. The administrator user account is equivalent to a Windows administrator account and provides access to all common services, FortiClient EMS for Chromebooks, and other application tasks. You can use this account to initially log into the server and to create other user accounts for normal day-to-day use of the applications.

It is recommended you install FortiClient EMS for Chromebooks on a dedicated server in a controlled environment. Installing other software applications can interfere with normal operation of FortiClient EMS for Chromebooks.

Downloading the installation file

FortiClient EMS for Chromebooks is available for download from the following location:

- Fortinet Support website: https://support.fortinet.com/

You can also receive the installation file from a sales representative.

The following installation file is available for FortiClient EMS for Chromebooks:

- `FortiClientEnterpriseManagement_Chromebook_1.2.1.<build>_x64.exe`

For information about obtaining FortiClient EMS for Chromebooks, contact your Fortinet reseller.

Installing FortiClient EMS for Chromebooks

The FortiClient EMS for Chromebooks installation package includes:

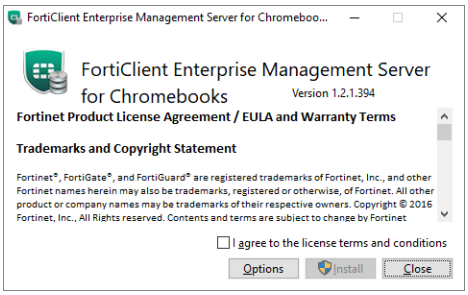
- FortiClient EMS for Chromebooks
- Microsoft SQL Server 2014 Express Edition
- Apache HTTP server

Local administrator rights and Internet access are required to install FortiClient EMS for Chromebooks.

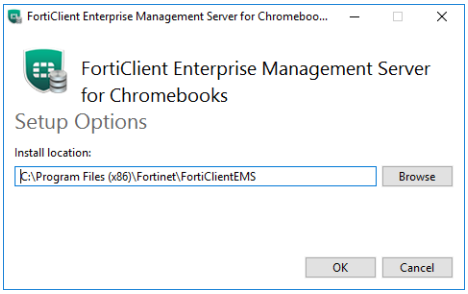
To install FortiClient EMS for Chromebooks:

1. If you are logged into the system as an administrator, double-click the downloaded installation file.
   If you are not logged in as an administrator, right-click the installation file, and select *Run as administrator*.

2. If applicable, select *Yes* in the *User Account Control* window to allow the program to make changes to your system.
3. In the installation window, select *I agree to the license terms and conditions* if you agree with the license terms and conditions. If you do not agree, you cannot install the software.

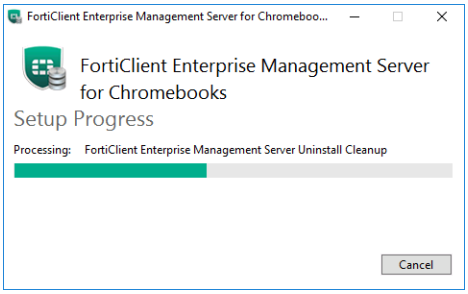


4. (Optional) Click *Options* to specify a custom directory for the FortiClient EMS for Chromebooks installation.

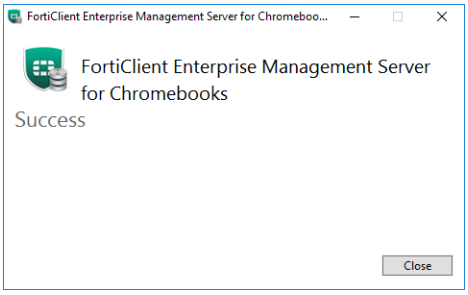


   a. Click *Browse* to locate and select the custom directory.
   b. Click *OK* to return to the installation wizard.
5. Click *Install*.

   The installation may take 30 minutes or longer. It may appear to stop at times, but this is only because certain steps in the installation process take longer than others.



6. When the program has installed correctly, the *Success* window displays. Click *Close*.



A *FortiClient Enterprise Management Server* icon is added to the desktop.

Starting FortiClient EMS for Chromebooks and logging in

FortiClient EMS for Chromebooks runs as a service on Windows computers.

To start FortiClient EMS for Chromebooks:

1. Double-click the *FortiClient Enterprise Management Server for Chromebooks* icon.
2. Sign in with the username *admin* and no password.
3. Change the username and password by going to *View* > *User Management* > *Administration*.
4. Configure FortiClient EMS for Chromebooks by going to *View* > *Settings*.

Accessing FortiClient EMS for Chromebooks remotely

You can access FortiClient EMS for Chromebooks remotely using a web browser instead of the GUI.

To enable remote access to FortiClient EMS for Chromebooks:

1. Go to *View* > *Settings*.
2. On the *Server Settings* tab, enable *Remote Administration HTTPS Access*.
3. In the *Custom Host Name* box, type the host name or IP address.
4. Click *Save*.

To remotely access FortiClient EMS for Chromebooks:

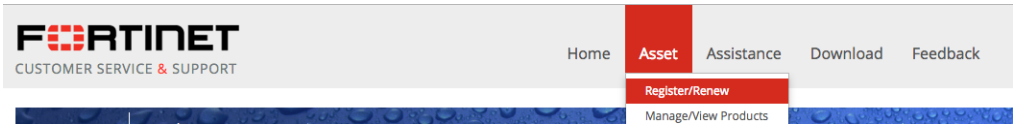
- To access EMS from the EMS server, visit `https://localhost`
- To access the server remotely, use the server's hostname: `https://<server_name>`
  Ensure you can ping `<server_name>` remotely. This can be achieved by adding it into a DNS entry or to the Windows hosts file. You may have to modify the Windows firewall rules to allow the connection.

Licensing FortiClient EMS for Chromebooks

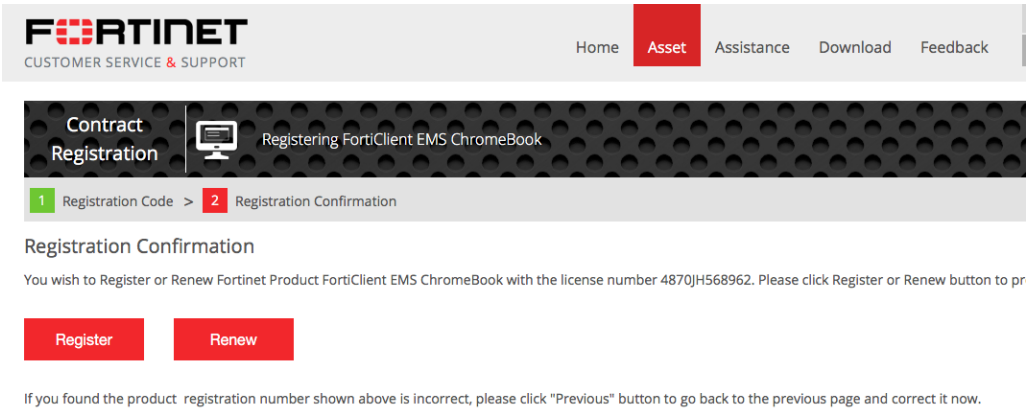
To license FortiClient EMS for Chromebooks:

1. Purchase FortiClient EMS for Chromebooks from a reseller.
   You can visit fortinet.com/partners.html to find a reseller. Once you purchase FortiClient EMS for Chromebooks, you receive the *Service Registration Document* via email. This email contains the *Contract Registration Code* used to obtain the FortiClient EMS for Chromebooks license.
2. Log into the Fortinet Support website.
3. Register FortiClient EMS for Chromebooks:

a. Go to *Asset* > *Register/Renew*.



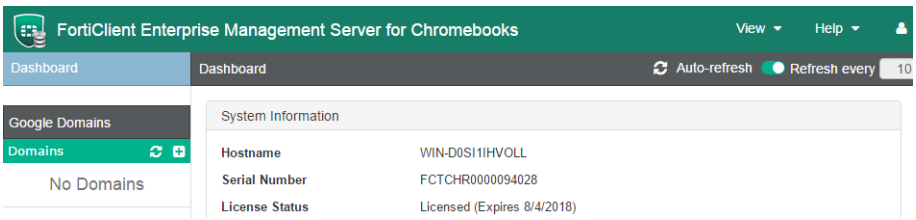
b. In the *Specify Registration Code* field, enter the *Contract Registration Code*. This is the number received in the license email from Fortinet.
c. Select the end user type, then click *Next*.
d. Click *Register*.



If you have not registered an EMS device, you are prompted to do so. This requires obtaining the *Hardware ID* from FortiClient EMS. You can obtain the *Hardware ID* by going to *Help* > *About* > *Hardware ID*.

e. In the *Product Description* field, enter a product description if desired, then enter the *Hardware ID*.
f. Select the *Fortinet Partner* reseller, then click *Next*.
g. Read, verify, and agree to the service's *Terms and Conditions*, then click *Next*.
h. Verify the *Product Entitlement* list for your FortiClient EMS for Chromebooks purchase. Select the *BY ACCEPTING THESE TERMS...* checkbox, then click *Confirm*. The license file is now available to use with your FortiClient EMS for Chromebooks installation.
i. Click *Finish*.

4. Retrieve the license key:
   a. Go to *Asset* > *Manage/View Products*. Select FortiClient EMS for Chromebooks.
   b. From the left panel, select *License & Key*.
   c. From the *Available Key(s)* list, click *Get The License File* for FortiClient EMS for Chromebooks.
5. License FortiClient EMS for Chromebooks:
   a. From FortiClient EMS for Chromebooks, go to *View* > *Upgrade License*, and click *Browse*.
   b. Select the license file and click *Upload File*. You have successfully licensed FortiClient EMS for Chromebooks.



To upgrade or renew your license, contact Fortinet Support.

License status

The *Dashboard* > *System Information* widget displays your license status. Your license status can change. The options are:

License Status	Description
Trial	If you just installed FortiClient EMS for Chromebooks, the trial license is enabled by default. You should upload the license file you purchased.
Non-expired license	You can upgrade the license. See License upgrades or renewals on page 61.
Expired license	You can renew the license. See License upgrades or renewals on page 61.

Extending license expiries

You can apply multiple licenses to FortiClient EMS for Chromebooks to extend the license expiry. For example, consider you purchase two one-year licenses for FortiClient EMS for Chromebooks. After you register and apply the first license, FortiClient EMS for Chromebooks has an expiry date of August 1, 2018. You can register and apply the second license as a renewal, after which FortiClient EMS for Chromebooks has an expiry date of August 1, 2019.

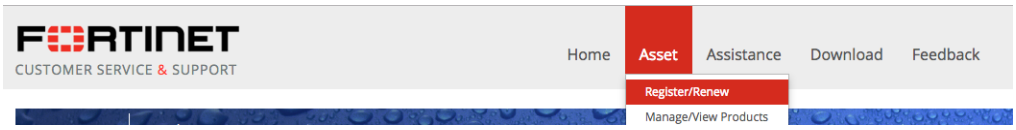
Note you must upload the second license file to FortiClient EMS for Chromebooks using the GUI. Registering the license does not automatically update the license expiry in FortiClient EMS for Chromebooks.

Using a second license to extend the license expiry date does not increase the number of licensed clients. To increase the number of licensed clients, contact Fortinet Support for a co-term contract.

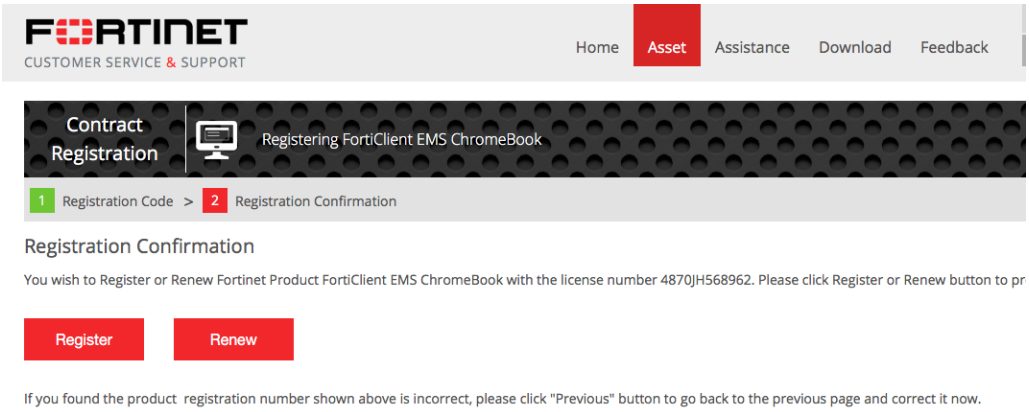
To extend a license expiry:

1. Purchase two FortiClient EMS for Chromebooks licenses separately from a reseller. You must purchase the licenses separately to ensure there are two registration codes. Otherwise, you cannot stack the licenses.

   You can visit fortinet.com/partners.html to find a reseller. Once you purchase FortiClient EMS for Chromebooks, you receive the *Service Registration Document* via email. This email contains the *Contract Registration Code* used to obtain the FortiClient EMS for Chromebooks license.
2. Register and apply the first license to FortiClient EMS for Chromebooks as described in Licensing FortiClient EMS for Chromebooks on page 20.
3. Register the second license:
   a. Log into the Fortinet Support website.
   b. Go to *Asset* > *Register/Renew*.

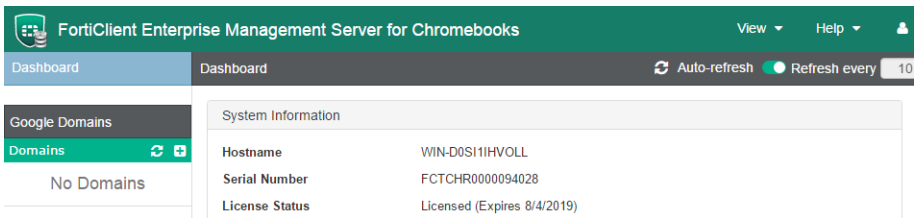


c. In the *Specify Registration Code* field, enter the *Contract Registration Code*. This is the number received in the license email from Fortinet.
d. Select the end user type, then click *Next*.
e. In the *Registration Confirmation* window, click *Renew*.



f. In the *Specify Fortinet Registration Information* window, do one of the following. You can find the serial number in the *System Information* widget in FortiClient EMS for Chromebooks.
    i. Enter the serial number in the *The Product Serial Number is* field.
    ii. Select the desired serial number in the *Product SN* list.
g. Read, verify, and agree to the service's *Terms and Conditions*.

4. Retrieve the license key:
    a. Go to *Asset* > *Manage/View Products*. Select FortiClient EMS for Chromebooks.
    b. From the left panel, select *License and Key*.
    c. From the *Available Key(s) List*, select the FortiClient EMS for Chromebooks entry. Then, click *Get The License File*.
5. License FortiClient EMS for Chromebooks:
    a. From FortiClient EMS for Chromebooks, go to *View* > *Upgrade License*, then click *Browse*.
    b. Select the license file and click *Upload File*. You have successfully extended the license for FortiClient EMS for Chromebooks. The expiry date displayed in the *System Information* widget updates to a year after the initial license expiry date.



Help with licensing

For licensing issues with FortiClient EMS for Chromebooks, contact the licensing team at Fortinet Technical Assistance Center (TAC):

- Phone: +1-866-648-4638
- Technical support: support.fortinet.com/

Specifying different ports

In cases where there are pre-existing services running on default FortiClient EMS for Chromebooks ports, you can specify another port using the CLI to run the installer. You can use the following command:

Command	Description
`RemoteManagementPort`	Port used for EMS administration.

Upgrading Microsoft SQL Server Express to Microsoft SQL Server Standard or Enterprise

FortiClient EMS for Chromebooks is installed with Microsoft SQL Server Express, which has a file size limit of 10 GB per database. Log entries recorded in the database are rotated on a schedule of seven days (one week) by default. If the FortiClient deployment is large, the database size may reach the 10 GB limit over time. The FortiClient EMS for Chromebooks administrator may upgrade SQL Server from Express to Standard or Enterprise edition. The database file size limit for these editions is in the PB range, which is unlimited for most practical usage.

Microsoft SQL Server Express is free. All other editions require a license from Microsoft.

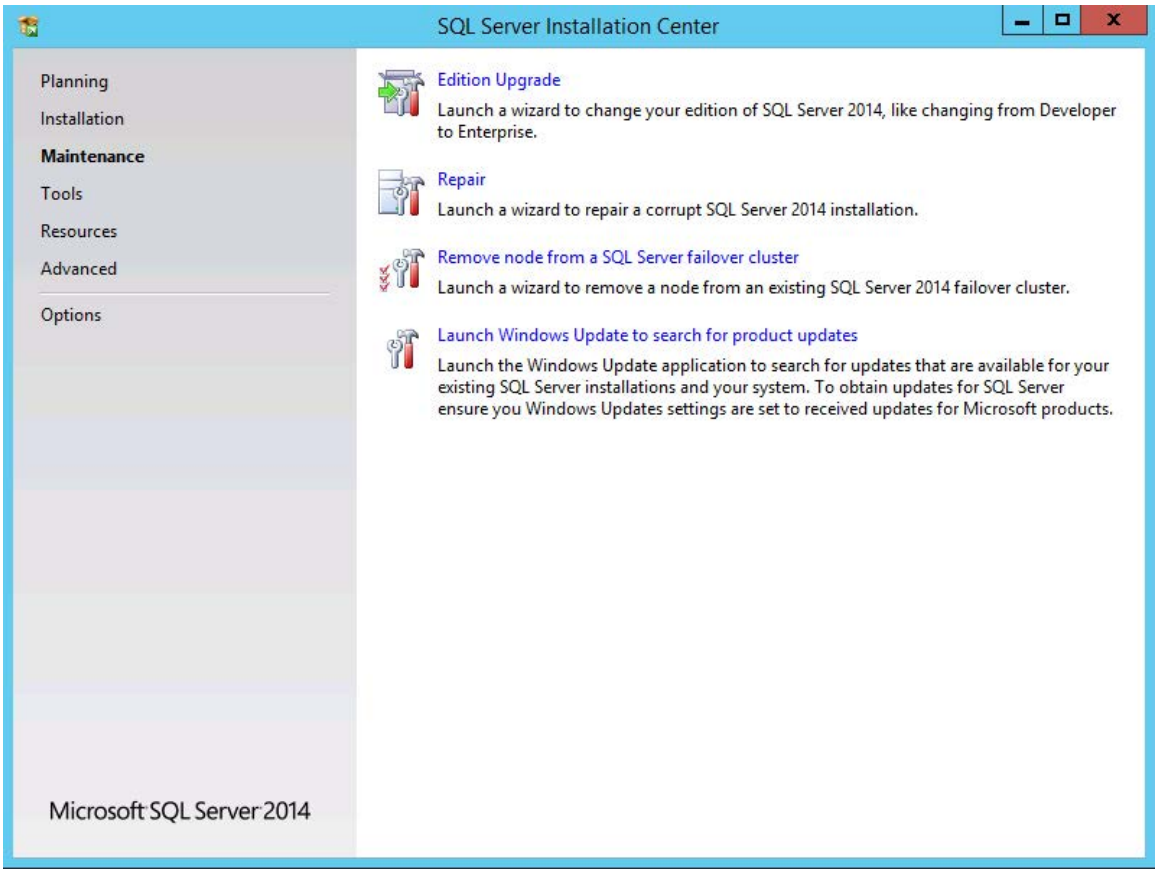
See the following Microsoft documentation on upgrading between editions called *Upgrade to a Different Edition of SQL Server 2014 (Setup)* at https://technet.microsoft.com/en-us/library/cc707783(v=sql.120).aspx

The EMS database is saved in the *C:\Program Files\Microsoft SQL Server\MSSQL12.FCEMS\MSSQL\DATA\FCM_root.mdf* file in the EMS host server. This file's size should remain below the 10 GB limit for Microsoft SQL Server Express.

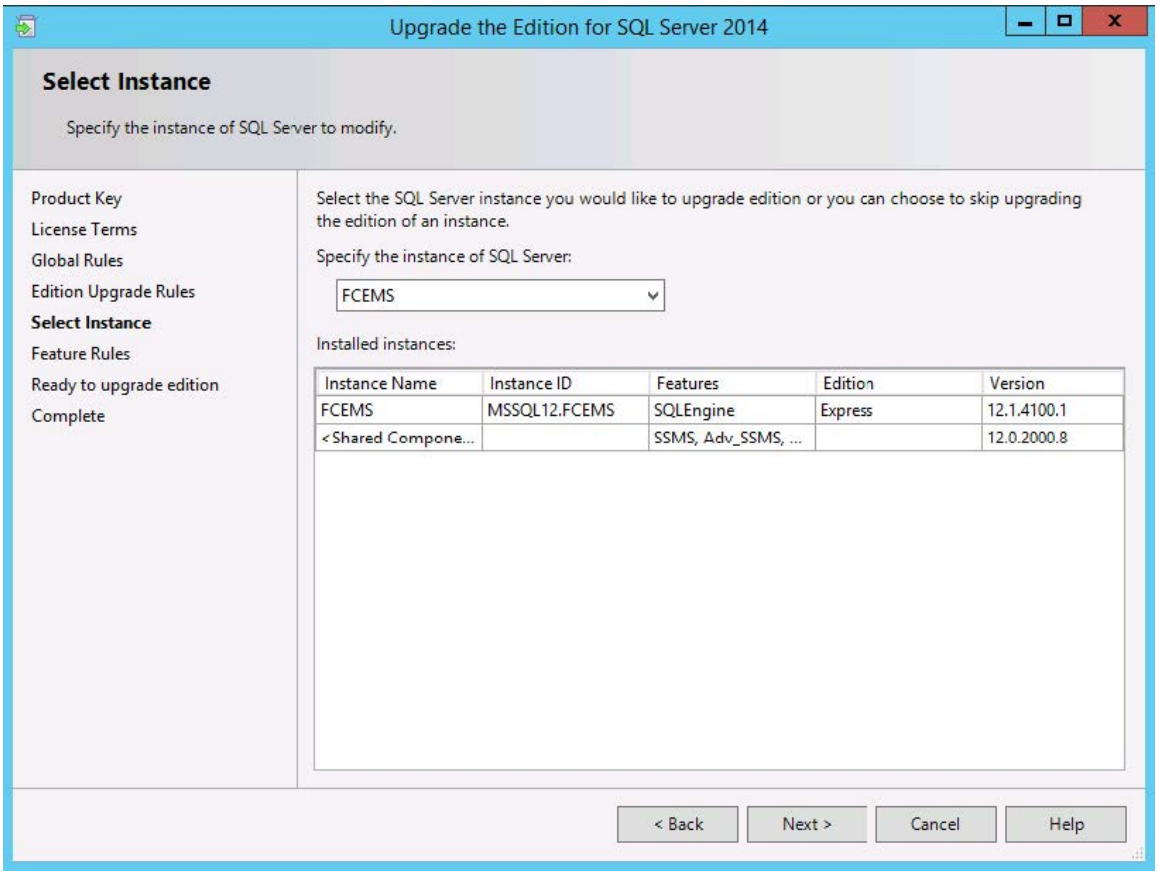
It is recommended to do a database edition upgrade outside normal production hours.

To upgrade Microsoft SQL Server Express:

1. Attach the SQL Server 2014 installation media to the FortiClient EMS for Chromebooks server.
   The installation media is a DVD or ISO file. If using the DVD, insert the DVD into the EMS host computer (host server). If your host server is a virtual machine, use the ISO file.
2. Run the SQL Server setup application wizard.
3. In the *SQL Server Installation Center* wizard, go to *Maintenance* > *Edition Upgrade*.



4. Enter the *product key*.
5. Accept the license terms, then click *Next*.
6. Under *Select Instance*, in the *Specify the instance of SQL Server* dropdown list, select *FCEMS*. Then, click *Next*.



7. Under *Ready to upgrade edition*, click *Upgrade*.
8. After the upgrade is complete, click *Finish*.

Testing the SQL server upgrade

It is recommended to run a short test on FortiClient EMS for Chromebooks after the upgrade to verify proper operations. A simple test may be to:

1. Register FortiClient on one or two test endpoints to FortiClient EMS for Chromebooks.
2. Create a new custom group in FortiClient EMS for Chromebooks and add the test endpoints to it.
3. Create a new endpoint profile and assign it to the new custom group.
4. Check that FortiClient on the test endpoints received the new profile.

Monitor the system closely over the first few days for any unusual behavior.

Uninstalling FortiClient EMS for Chromebooks

Use the *Programs and Features* pane of the Microsoft Windows Control Panel to uninstall FortiClient EMS for Chromebooks.

FortiClient EMS for Chromebooks installs the following dependencies. If other applications on the same computer are not using them, you can uninstall them manually after removing FortiClient EMS for Chromebooks.

- Microsoft ODBC Driver 11 for SQL Server
- Microsoft SQL Server 2008 Setup Support Files
- Microsoft SQL Server 2012 Native Client
- Microsoft SQL Server 2014 (64-bit)
- Microsoft SQL Server 2014 Setup (English)
- Microsoft SQL Server 2014 Transact-SQL ScriptDom
- Microsoft Visual C++ 2010 x64 Redistributable – 10.0
- Microsoft Visual C++ 2010 x86 Redistributable – 10.0
- Microsoft Visual C++ 2013 x86 Redistributable – 12.0
- Microsoft VSS Writer for SQL Server 2014
- SQL Server Browser for SQL Server 2014

To uninstall FortiClient EMS for Chromebooks:

1. Select *Start* > *Control Panel* > *Programs* > *Uninstall a program*.
2. Select *FortiClient Enterprise Management Server*, and click *Uninstall*.
3. Follow the uninstallation wizard prompts.

Google Admin Console Setup

This section describes how to add and configure the FortiClient Web Filter extension on Chromebooks enrolled in the Google domain.

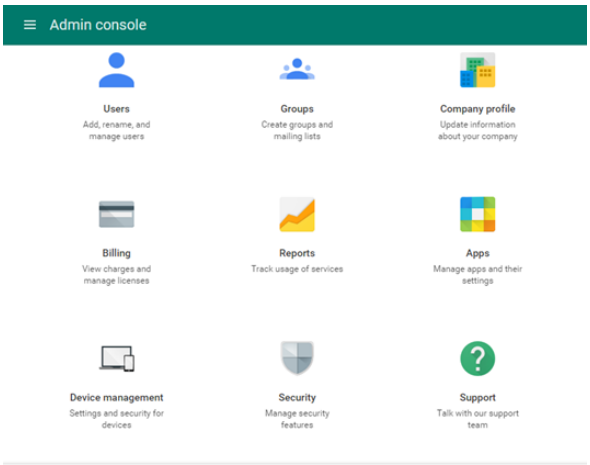
Following is a summary of how to set up the Google Admin console:

1. Log into the Google Admin console. See Logging into the Google Admin console on page 28.
2. Add the FortiClient Web Filter extension. See Adding the FortiClient Web Filter extension on page 28.
3. Configure the FortiClient Web Filter extension. See Configuring the FortiClient Web Filter extension on page 29.
4. Add the root certificate. See Adding root certificates on page 30.

Logging into the Google Admin console

To log into the Google Admin console:

1. Log into the Google Admin console (https://admin.google.com) using your Google domain admin account. The Admin console displays.



Adding the FortiClient Web Filter extension

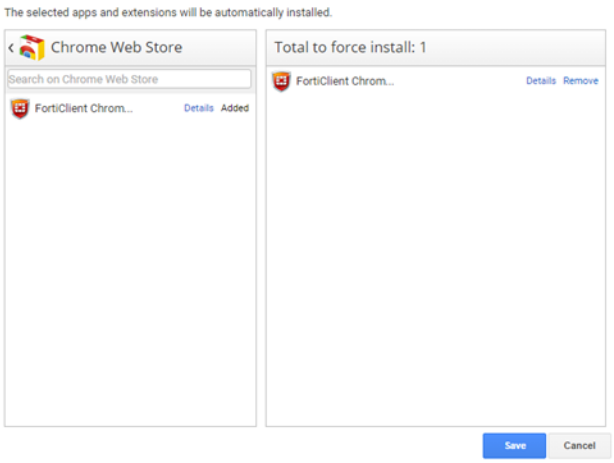
FortiClient EMS for Chromebooks software is not available for public use. You can only enable the feature using the following extension ID: igbgpehnbmhgdgjbhkkpedommgmfbeao

Note that if the FortiClient Web Filter extension is pushed to Chromebooks enrolled in the Google domain, the extension is also installed on Windows and OS X devices when the user uses their Google single sign-on

credentials to log into the Chrome browser on that device. The downloaded FortiClient Web Filter extension makes the Chrome browser unusable on the Windows or OS X device.

To add the FortiClient Web Filter extension:

1. In the Google Admin console, go to *Device management* > *Chrome Management* > *User Settings* > *Apps and Extensions* > *Force-installed Apps and Extensions* > *Manage force-installed apps*.
2. Select *Chrome Web Store*, and search for the following extension ID: igbgpehnbmhgdgjbhkkpedommgmfbeao.
3. Add the extension ID and save.
   The extension name displays as *FortiClient Chromebook Web Filter Extension*.



Configuring the FortiClient Web Filter extension

You must configure the FortiClient Chromebook Web Filter extension to enable the Google Admin console to communicate with FortiClient EMS for Chromebooks.

FortiClient EMS for Chromebooks hosts the services that assign endpoint profiles of web filtering policies to groups in the Google domain. FortiClient EMS for Chromebooks also handles the logs and web access statistics sent from the FortiClient Web Filter extension.

FortiClient EMS for Chromebooks is the profile server.

To configure the FortiClient Web Filter extension:

1. In FortiClient EMS for Chromebooks, locate the server name and port by going to *View* > *Settings*.
2. Create a text file that contains the following text:

```
{
   "ProfileServerUrl": { "Value": "https://< ProfileServer >:< port for Profile Server >"}
}
```

   For example:

```
{
   "ProfileServerUrl": { "Value": "https://ems.mydomain.com:8443”}
}
```

3. In the Google Admin console, go to *Device management* > *Chrome Management* > *App Management* > *FortiClient Chrome Web Filter Extension* > *User settings*.
4. Click a domain or organization unit (OU).
5. In the right pane, under *Configure*, upload a new configuration file.
   You can also view the current settings.
6. Click *Save*.
7. Go to *Device Management* > *Chrome* > *App Management* to view your configured Chrome apps.

Adding root certificates

This section includes the following information:

Communication with the FortiClient Chromebook Web Filter extension

The FortiClient Chromebook Web Filter extension communicates with FortiClient EMS for Chromebooks using HTTPS connections. The HTTPS connections require an SSL certificate. You must obtain an SSL certificate and add it to FortiClient EMS for Chromebooks to allow the extension to trust FortiClient EMS for Chromebooks.

If you use a public SSL certificate, you only need to add the public SSL certificate to FortiClient EMS for Chromebooks. See Adding SSL certificates to FortiClient EMS for Chromebooks on page 65.

However, if you prefer to use a certificate not from a common CA, you must add the SSL certificate to FortiClient EMS for Chromebooks and push your certificate's root CA to the Google Chromebooks. Otherwise, the HTTPS connection between the FortiClient Chromebook Web Filter extension and FortiClient EMS for Chromebooks will not work. See Uploading root certificates to the Google Admin console on page 32.

Communication with FortiAnalyzer for logging

This section applies only if you are sending logs from FortiClient EMS for Chromebooks to FortiAnalyzer. If you are not sending logs, skip this section.

Sending logs to FortiAnalyzer requires you enable ADOMs in FortiAnalyzer and add FortiClient EMS for Chromebooks to FortiAnalyzer. FortiClient EMS for Chromebooks is added as a device to the FortiClient ADOM in FortiAnalyzer. See the *FortiAnalyzer Administration Guide*.

FortiClient EMS for Chromebooks supports logging to FortiAnalyzer. If you have a FortiAnalyzer device and configure FortiClient EMS for Chromebooks to send logs to FortiAnalyzer, a FortiAnalyzer CLI command must be enabled and an SSL certificate is required to support communication between the FortiClient Web Filter extension and FortiAnalyzer.

If you use a public SSL certificate, you only need to add the public SSL certificate to FortiAnalyzer. See Adding SSL certificates to FortiAnalyzer on page 31.

However, if you prefer to use a certificate not from a common CA, you must add the SSL certificate to FortiAnalyzer and push your certificate's root CA to the Google Chromebooks. Otherwise, the HTTPS connection between the FortiClient Chromebook Web Filter extension and FortiAnalyzer will not work. See Uploading root certificates to the Google Admin console on page 32.

The FortiAnalyzer IP address should be specified in the SSL certificate. If you're using a public SSL certificate, the FortiAnalyzer IP address can be assigned to *Common Name* or *Alternative Name*. If you're using a self-signed (nonpublic) SSL certificate, your certificate's *Subject Alternative Name* must include `IP:<FortiAnalyzer IP>`.

Enabling HTTP and HTTPS logging access to FortiAnalyzer

You must use the FortiAnalyzer CLI to add HTTP-logging and HTTPS-logging to the allow-access list in FortiAnalyzer. This command is one step in the process that allows FortiAnalyzer to receive logs from FortiClient EMS for Chromebooks.

In FortiAnalyzer CLI, enter the following command:

```
config system interface
   edit "port1"
      set allowaccess https ssh http http-logging https-logging
   next
end
```

Adding SSL certificates to FortiAnalyzer

To add SSL certificates to FortiAnalyzer:

1. In FortiAnalyzer, go to *System Settings* > *Certificates* > *Local Certificates*.
2. Click *Import*. The *Import Local Certificate* dialog appears.
3. In the *Type* list, select *Certificate* or *PKCS #12 Certificate*.
4. Beside *Certificate File*, click *Browse* to select the certificate.
5. Enter the password and certificate name.
6. Click *OK*.

Selecting certificates for HTTPS connections

To select certificates for HTTPS connections:

1. In FortiAnalyzer, go to *System Settings* > *Admin* > *Admin Settings*.
2. In the *HTTPS & Web Service Certificate* box, select the certificate to use for HTTPS connections, and click *Apply*.

Summary of where to add certificates

The following table summarizes where to add certificates to support communication with the FortiClient Web Filter extension and FortiAnalyzer.

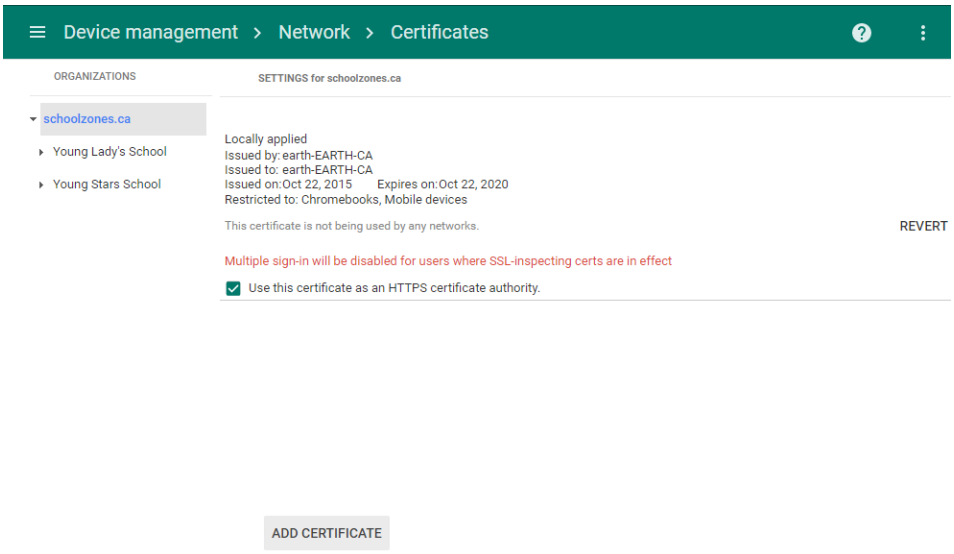
Scenario	Certificate and CA	Where to Add Certificates
Allow the FortiClient Chromebook Web Filter extension to trust EMS	Public SSL certificate	• Add SSL certificate to FortiClient EMS for Chromebooks.
	SSL certificate not from a common CA	• Add SSL certificate to FortiClient EMS for Chromebooks. • Add your certificate's root CA to the Google Admin console.
Allow the FortiClient Chromebook Web Filter extension to trust FortiAnalyzer for logging	Public SSL certificate	• Add SSL certificate to FortiAnalyzer.
	SSL certificate not from a common CA	• Add SSL certificate to FortiAnalyzer. • Add your certificate's root CA to the Google Admin console.

Uploading root certificates to the Google Admin console

To add root certificates:

1. In the Google Admin console, go to *Device Management* > *Network* > *Certificates (root certificate) (crt certificate)*.
2. Add the root certificate.
3. Select the *Use this certificate as an HTTPS certificate authority* checkbox.

Do not forget to select the *Use this certificate as an HTTPS certificate authority* checkbox.



Disabling access to Chrome developer tools

It is recommended to disable access to Chrome developer tools. This blocks users from disabling the FortiClient Web Filter extension.

To disable access to Chrome developer tools:

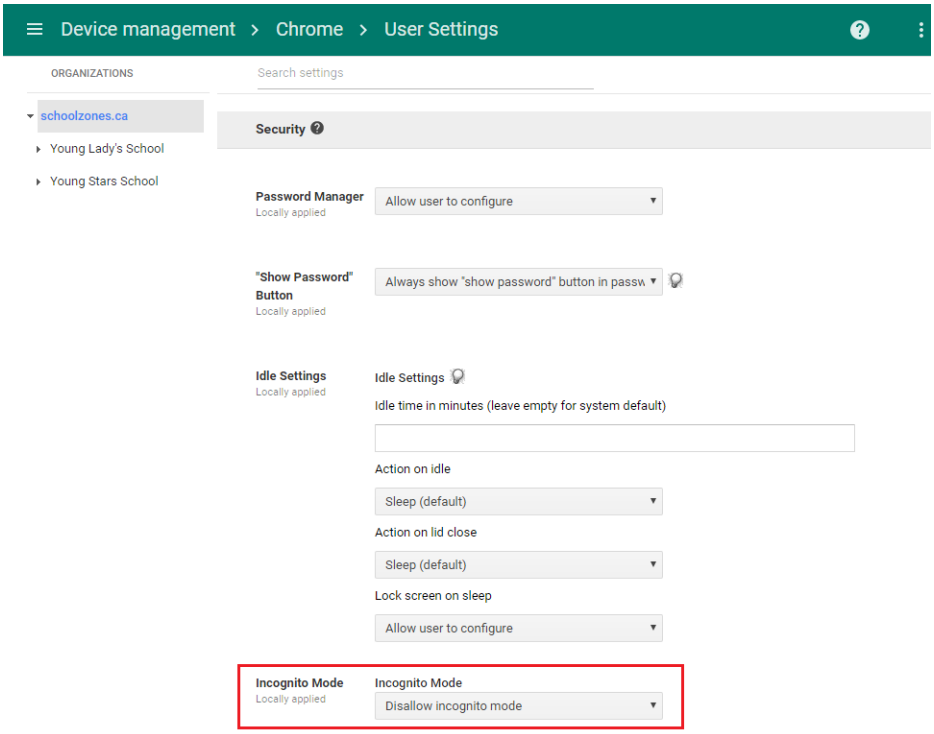
1. In the Google Admin console, go to *Device management* > *Chrome Management* > *User Settings*.
2. For the *Developer Tools* option, select *Never allow use of built-in developer tools*.

Disallowing incognito mode

When users browse in incognito mode, extensions are bypassed. Incognito mode should be disallowed for managed Google domains.

To disallow incognito mode:

1. In the Google Admin console, go to *Device management* > *Chrome management* > *User settings*.
2. From the left panel, select the organization.
3. In the *Security* section, set *Incognito Mode* to *Disallow incognito mode*.



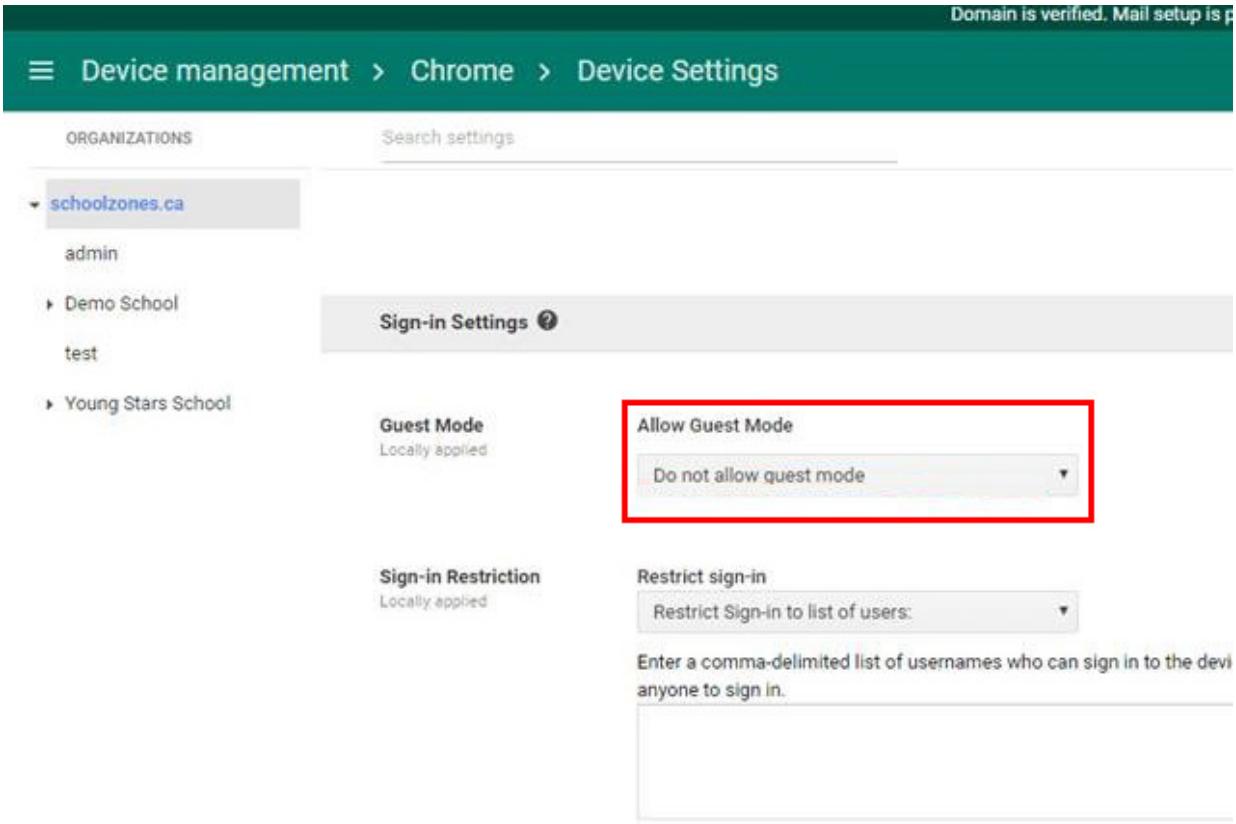
4. Click *Save*.

Disallowing guest mode

Guest mode should be disallowed for managed Google domains.

To disallow guest mode:

1. In the Google Admin console, go to *Device management* > *Chrome management* > *Device settings* > *Sign-in settings*.
2. From the left panel, select the organization.
3. Under *Guest Mode*, select *Do not allow guest mode* from the *Allow Guest Mode* dropdown list.



4. Click *Save*.

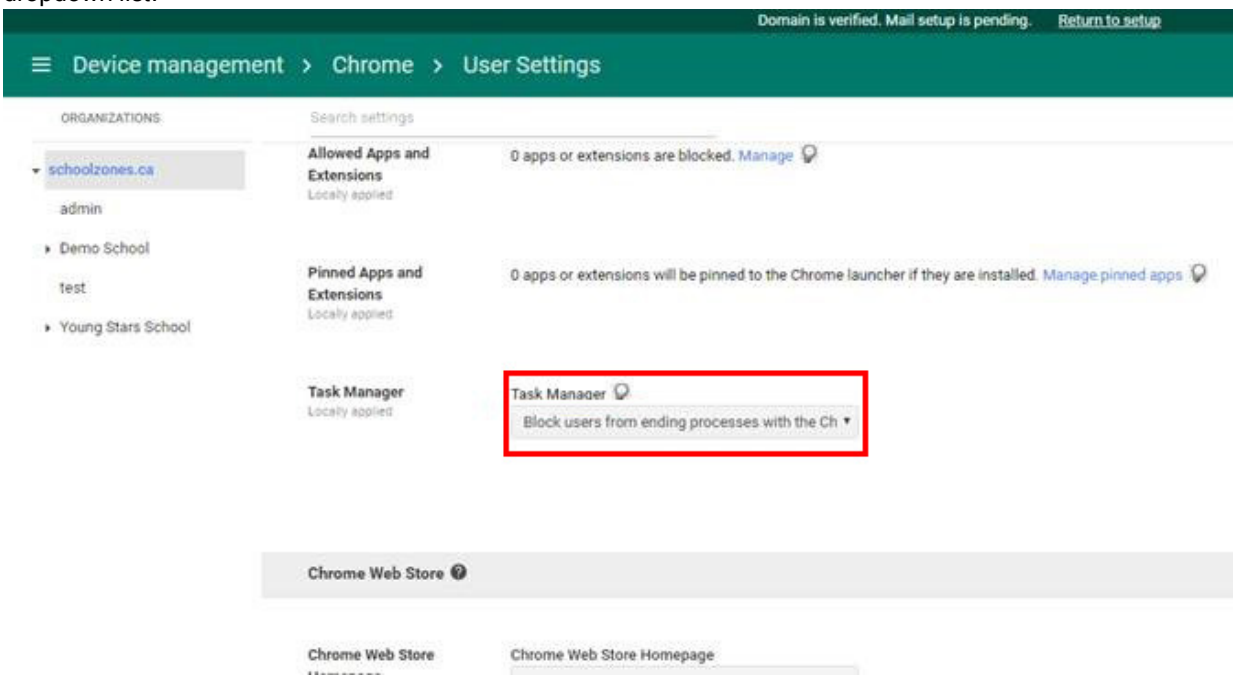
Blocking Task Manager

Task Manager should be blocked for managed Google domains.

To block Task Manager:

1. In the Google Admin console, go to *Device Management* > *Chrome Management* > *User settings* > *Apps and Extensions*.

2. From the left panel, select the organization.
3. Under *Task Manager* select *Block users from ending processes with the Chrome Task Manager* from the dropdown list.



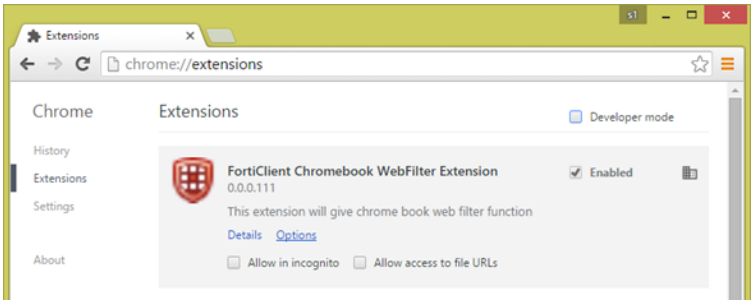
4. Click *Save*.

Verifying the FortiClient Web Filter extension

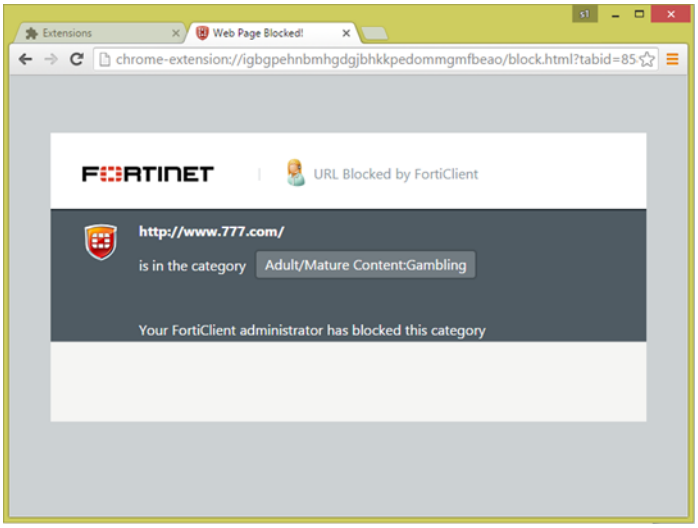
After you add the Google domain to FortiClient EMS for Chromebooks, the Google Admin console automatically pushes the FortiClient Web Filter extension to the Chromebooks when users log into the Google domain. You can verify the feature is available in Chromebooks.

To verify that the extension is installed:

1. Open the Google Chrome browser.
2. Type the following in the address bar: *chrome://extensions*



3. Visit any gambling site, such as http://www.777.com, and confirm the site is blocked.



Service Account Credentials

FortiClient EMS for Chromebooks requires service account credentials generated by the Google Developer console. You can use the default service account credentials provided with FortiClient EMS for Chromebooks or generate and use unique service account credentials, which is more secure.

The service account credentials must be the same in FortiClient EMS for Chromebooks and the Google Admin console.

This section describes how to configure default and unique service account credentials. See the following sections:

- Configuring default service account credentials on page 37
- Configuring unique service account credentials on page 38

Configuring default service account credentials

FortiClient EMS for Chromebooks includes the following default service account credentials generated by the Google Developer console:

Option	Default Setting	Where Used
Client ID	102515977741391213738	Google Admin console
Email address	account-1@forticlientwebfilter.iam.gserviceaccount.com	FortiClient EMS for Chromebooks
Service account certificate	A certificate in `.pem` format for the service account credentials	FortiClient EMS for Chromebooks

The service account credentials are a set. If you change one credential, you must change the other two credentials.

Adding the default service account client ID to the Google Admin console

To configure the default service account credentials, you must add the client ID's default value to the Google Admin console. No other configuration for service account credentials is required. See Adding service account credentials to the Google Admin console on page 41.

Configuring unique service account credentials

When using unique service account credentials for improved security, you must complete the following steps to add the unique service account credentials to the Google Admin console and FortiClient EMS for Chromebooks:

1. Create unique service account credentials using the Google Developer console. See Creating unique service account credentials on page 38.
2. Add the unique service account credentials to the Google Admin console. See Adding service account credentials to the Google Admin console on page 41.
3. Add the unique service account credentials to FortiClient EMS for Chromebooks. See Adding service account credentials to EMS on page 42.

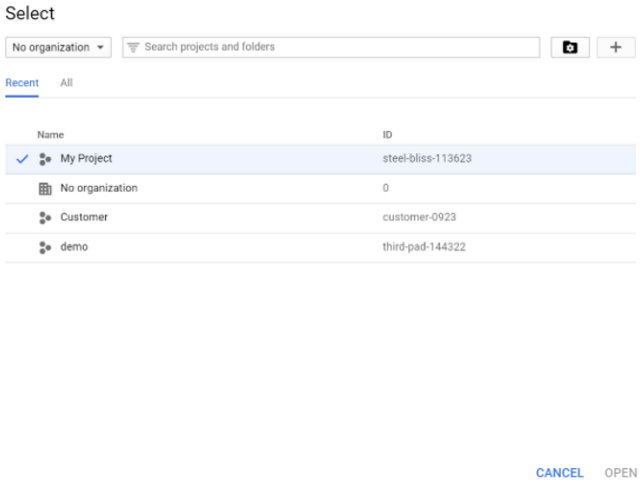
Creating unique service account credentials

Creating a unique set of service account credentials provides more security. Unique service account credentials include the following:

- Client ID (a long number)
- Service account ID (email address)
- Service account certificate (a certificate in `.pem` format)

To create a unique service account:

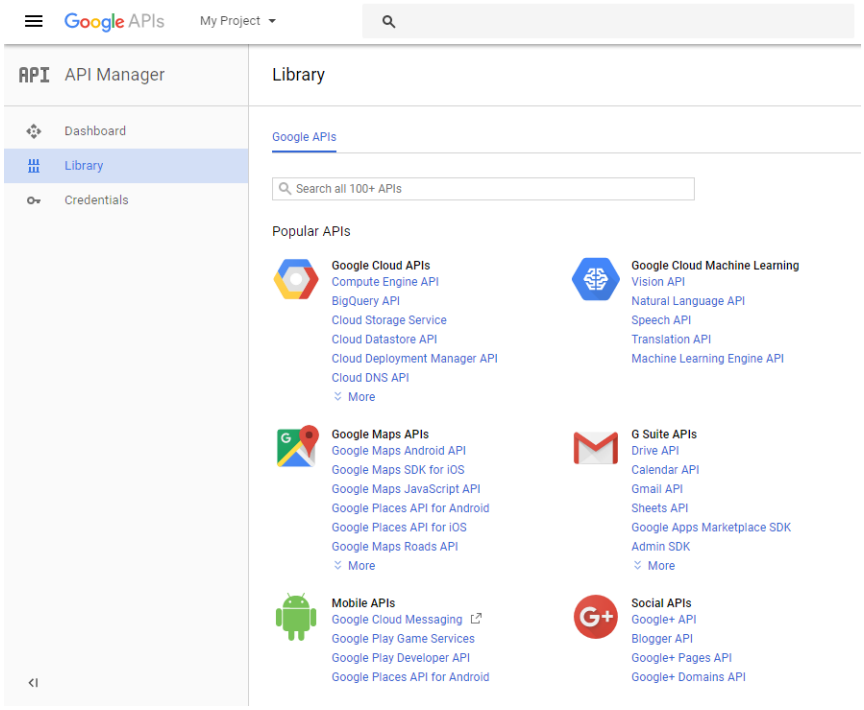
1. Go to https://console.developers.google.com.
2. Log in with your Google for Work account credentials.
3. Create a new project:
   a. Click the toolbar list. The browser displays the following dialog.



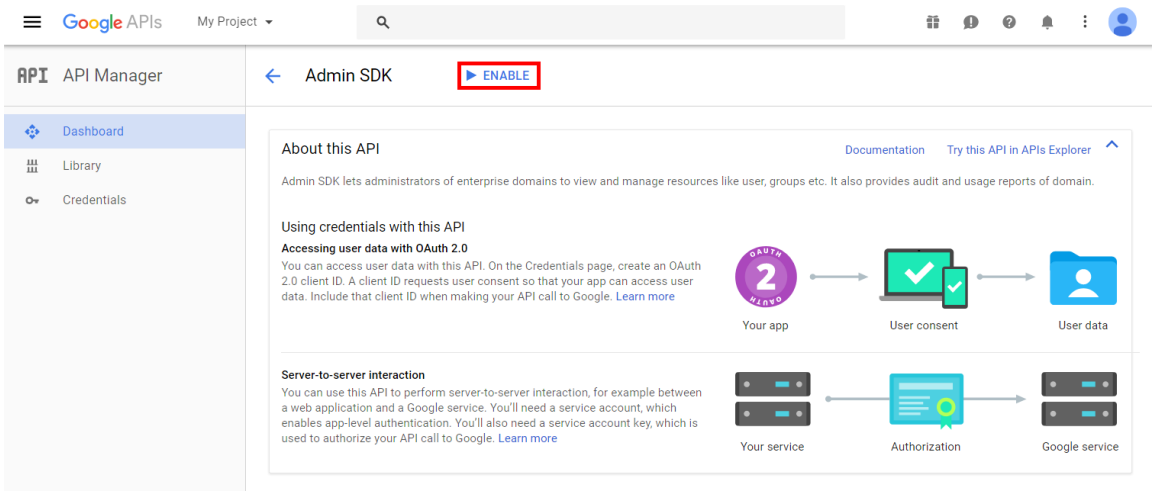
   b. Select your organization, if you see an organization dropdown list.
   c. Click the + button.
   d. In the *Project name* field, enter your project name, then click *Create*.
4. Enable the Admin SDK:

a. Select your project from the toolbar list, then go to the *Library* tab.

b. Under *G Suite APIs*, click *Admin SDK*.



c. Click *ENABLE*.



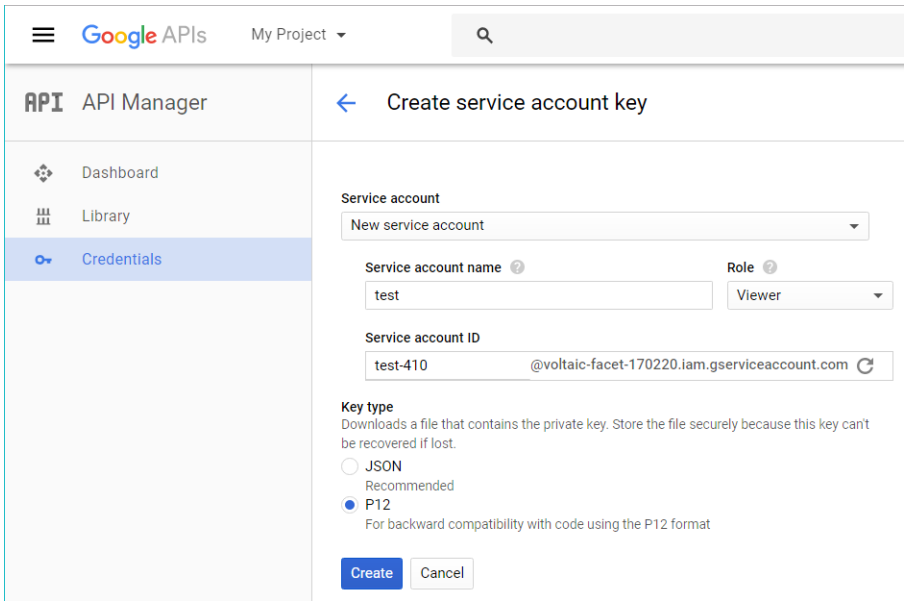
5. Create a service account:

a. Go to the *Credentials* tab and select *Create Credentials* > *Service account key*.

b. From the *Service account* list, select *New Service Account*. Enter a service account name.

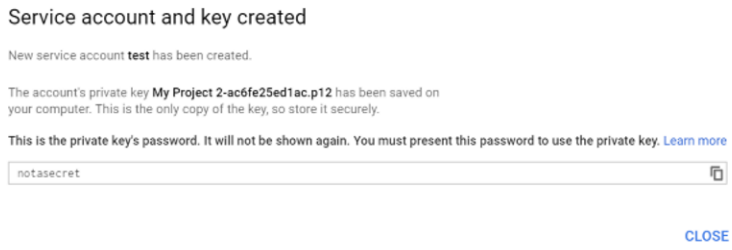
c. From the *Role* list, select *Project* > *Viewer*.

d. Select *P12* as the *Key type* and click *Create*.

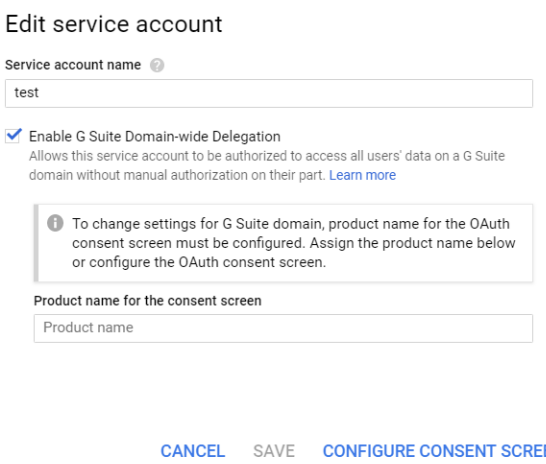


After you create the service account, a private key with the `P12` extension is saved on your computer.

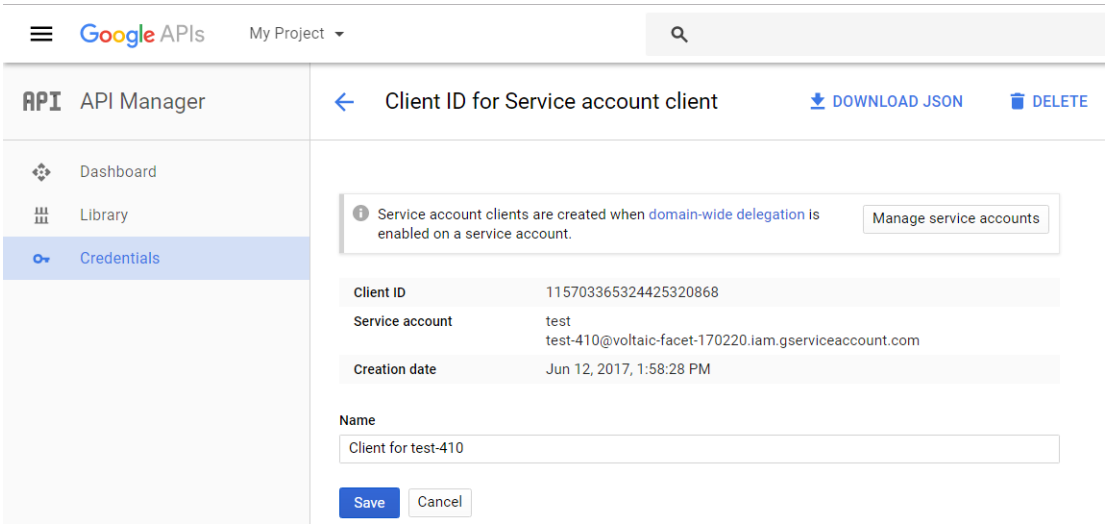
> ⚠ The private key with the `P12` extension is the only copy you will receive. Keep it in a safe place. You should also remember the password prompted on the screen. At this time, that password should be **`notasecret`**.



6. Go to the *Credentials* page > *Manage service accounts*.
7. *Edit* the service account you just created and select the *Enable Google Apps Domain-Wide Delegation* checkbox. Enter a *Product name for the consent screen* if this field appears.



8. Click *Save*.
9. Click *View Client ID* to see your service account information. Record the client ID, service account, and the associated private key (downloaded in step 5d).



To use the private key in EMS, it needs to be converted to `.pem` format. You can use the following `openssl` command to convert it. Remember to use the notasecret password.

```
C:\OpenSSL-Win64\bin>openssl pkcs12 -in demo-
    976b9d6e9328.p12 -out serviceAccount-demo.pem -nodes -
    nocerts
Enter Import Password:
```

Adding service account credentials to the Google Admin console

This section describes how to add the client ID from the service account credentials to the Google Admin console. These settings allow Google to trust FortiClient EMS for Chromebooks, which enables FortiClient EMS for Chromebooks to retrieve information from the Google domain.

To add the client ID:

1. In the Google Admin console, go to *Security* > *Advanced settings* > *(you may need to click "show more" to see this)* > *Manage API client access*.
2. Set the following options:
   a. For the *Client Name* option, add the client ID from the service account credentials.
   b. For the *API Scopes* option, add the following string:
   https://www.googleapis.com/auth/admin.directory.orgunit.readonly,https://www.googleapis.com/auth/admin.directory.user.readonly

The API scopes are case-sensitive and must be lowercase. You may need to copy the string into a text editor and remove spaces created by words wrapping to the second line in the PDF.

3. Click *Authorize*.

Adding service account credentials to EMS

The section describes how to add the service account ID and service account certificate from the service account credentials to FortiClient EMS for Chromebooks.

To add service account credentials:

1. In FortiClient EMS for Chromebooks, go to *View* > *Settings*.
2. Click *EMS for Chromebook*, and set the following options:

The default service account credentials display. Overwrite the default settings with the unique set of service account credentials received from Fortinet.

Service Account ID	Displays the configured email address provided for the service account credentials.
New Service Account ID	Type a new email address for the service account credentials.
New Service Account Private Key	Click *Browse* and select the certificate provided with the service account credentials.

3. Click *Save*.
4. Update the client ID in the Google Admin console.

The service account credentials are a set. If you change one credential, you must change the other two credentials.

GUI

The FortiClient EMS for Chromebooks GUI consists of the following areas:

- Banner
- Left pane
- Content pane

Banner

Option	Description
License information	Displays current license status and number of licenses.
View	View and configure the following: • Upgrade License • User Management • Database Management • View Logs • Settings
Help	View the following: • Technical Documentation • How-To Videos • Forums • Getting Started • Create Support Package • About
<Logged in username>	Click the dropdown list beside the <logged in username> to log out of FortiClient EMS for Chromebooks.

Left pane

The left navigation pane is used to display content in the right content pane.

Option	Description
Dashboard	Displays a dashboard of information about all managed endpoints.
Google Domains	Add and manage Google domains.

Option	Description
Endpoint Profiles	Create and assign profiles and manage profile updates.

Content pane

The right content pane displays the user interface controls that correspond to the selection made in the left pane. The status and menu icons in the top-right display controls what you can use to configure additional settings for user management and each individual endpoint.

Dashboard

You can use the Dashboard to view summary information about the system and endpoints.

Viewing the Dashboard

To view the Dashboard:

1. In the left pane, click *Dashboard*.
   A *System Information* widget and charts and widgets of summary information display. See System Information widget on page 45 and Dashboard charts and widgets on page 46.
2. Click an event summary.
   The list of endpoints for the summary displays.
3. Click the *Back* button to return to the *Dashboard*.
4. Click a pie chart.
   The *Endpoints* content pane displays with more details about the endpoints related to the pie charts.

System Information widget

The following information displays in the *System Information* widget:

Option	Description
Hostname	Name of the computer on which FortiClient EMS for Chromebooks is installed.
Serial Number	Serial number for FortiClient EMS for Chromebooks.
License Status	Status of the license for FortiClient EMS for Chromebooks. See also Licensing FortiClient EMS for Chromebooks on page 20.
Used Licenses	Number of used licenses out of the total number of available licenses. Also displays a button for entering, upgrading, or renewing a license, depending on the license status. If you have just installed EMS, click the *Enter License* button to upload your license file. If you have a non-expired license, but want to upgrade your license, click the *Upgrade* button to upgrade your license file. If your current license is expiring, the *Renew* button is enabled for you to upload your new license file.
System Time	Time and date used by the computer on which FortiClient EMS for Chromebooks is installed.

Option	Description
System Database	Options to back up and restore the database. Click *Backup* to back up the database. Click *Restore* to restore a backed up database.
Current Admin	Name of the administrator logged into FortiClient EMS for Chromebooks.
Uptime	Number of days, hours, minutes, and seconds FortiClient EMS for Chromebooks has been running.

Dashboard charts and widgets

The Dashboard displays a number of pie charts. Each pie chart provides a summary of endpoint information. The sections in each chart are links. You can click any section of the pie charts or any row in the table to display more details.

Option	Description
Client Stats	Statistics of clients in use. The value entered in the *Settings* > *Log Settings* > *Auto Remove Web Filter Logs* determines this widget's data. • Managed and Unmanaged • Online and Offline • On-Net and Off-Net
Top 10 Webfilter Violations by Category (Past <number> Days)	The chart displays the top ten web filter violations by category in the past few days. You can configure the number of days. Go to *View* > *Settings* > *Log Settings*.
Top 10 Webfilter Violation by User (Past <number> Days)	The chart displays the top ten web filter violations a user has made in the past few days. You can configure the number of days. Go to *View* > *Settings* > *Log Settings*.
Top 10 Site Categories by Distribution (Past <number> Days)	The chart displays the distribution of top ten site categories in the past few days. You can configure the number of days. Go to *View* > *Settings* > *Log Settings*.
Blocked Sites Distribution (Past <number> Days)	The chart displays the distribution of blocked sites in the past few days. You can configure the number of days. Go to *View* > *Settings* > *Log Settings*.
Blocked Site Logs (Past <number> Days)	The chart displays the distribution of blocked site logs in the past few days. You can configure the number of days. Go to *View* > *Settings* > *Log Settings*.

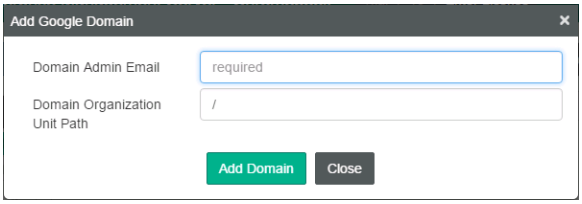
Domains

FortiClient EMS for Chromebooks needs to determine which devices to manage. Device information comes from the Google Admin console.

Adding Google domains

To add Google domains:

1. Go to *Google Domains*, and click the *Add a new Google domain* icon (the + button). The *Add Google Domain* dialog displays.



2. In the *Domain Admin Email* box, type your Google domain admin email.
3. In the *Domain Organization Unit Path* box, type the domain organization unit path.

> / stands for the root of the domain.

4. Click *Add Domain*.
   The Google domain information and users are imported into FortiClient EMS for Chromebooks.

Viewing domains

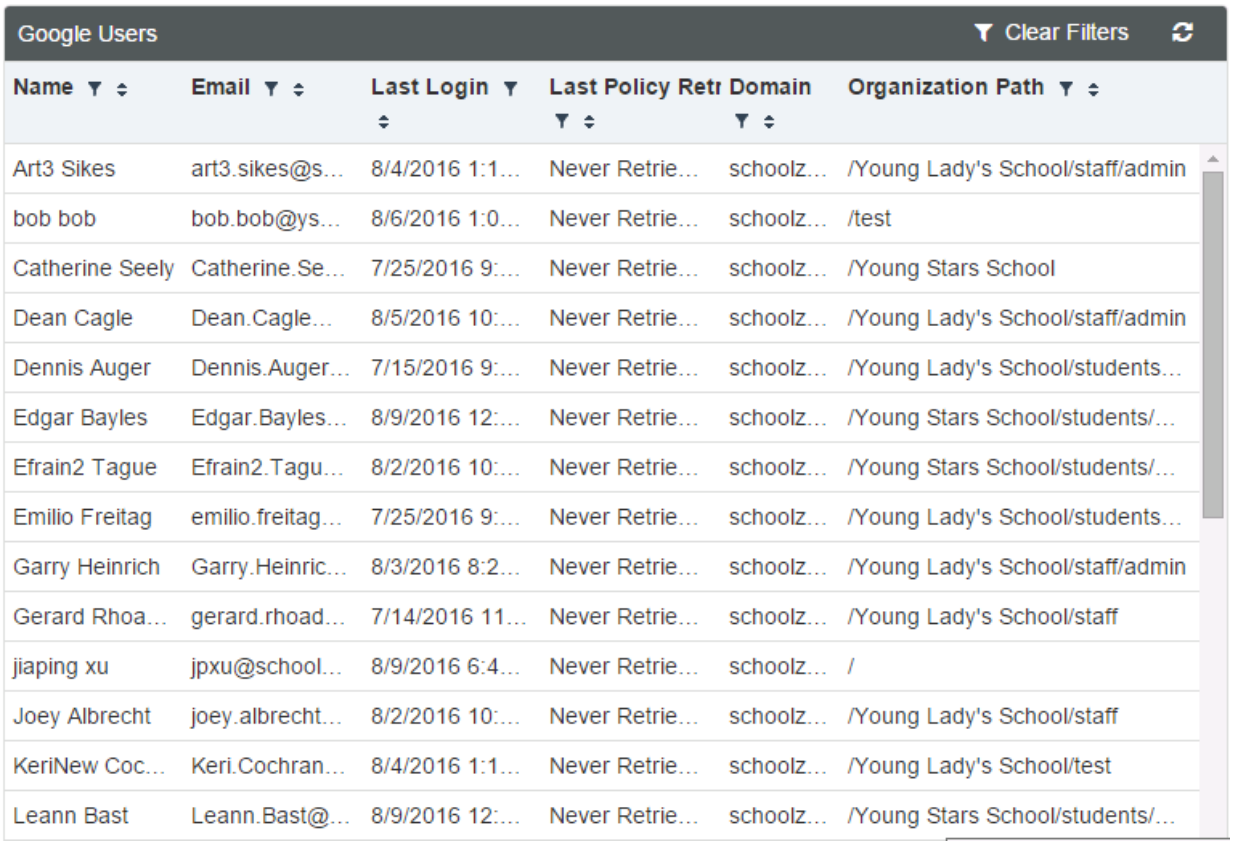
After you add domains to FortiClient EMS for Chromebooks, you can view the list of domains in *Google Domains*. You can also view the list of Google users in each domain and details about each Google user in the *User Details*, *Client Statistics*, and *Blocked Sites* panes.

Viewing the Google Users pane

You can view Google users' information in FortiClient EMS for Chromebooks.

To view the Google Users pane:

1. Go to *Google Domains* > *Domains* and click a domain. The list of Google users displays.



The following options are available in the toolbar:

Clear Filter (filter icon)	Click the Clear Current Filter icon to clear the currently used filter.
Refresh	Click the Refresh icon to refresh the page.

The following columns of information are displayed for Google users:

Name	Chromebook user's name.
Email	Chromebook user's email address.
Last Login	Date and time when the user last logged into the domain.
Last Policy Retrieval	Date and time of the last endpoint profile retrieved by the Google Chromebook.
Domain	Name of the domain to which the user belongs.
Organizational Path	Organization path in the domain.

Viewing user details

You can view details about each user in a Google domain.

To view user details:

1. Go to *Google Domains* > *Domains*. The list of domains displays.
2. Click a domain. The list of Google users displays.
3. Click a Google user and scroll to the bottom of the content pane. The *User Details*, *Client Statistics*, and *Blocked Sites* panes display.

User Details

Field	Information
Name	User's name.
Email	User's email address.
Last Login	Date and time when the user last logged into the domain.
Last Policy Retrieval	Date and time of the last endpoint profile retrieved by the Google Chromebook.
Organization Path	Organization path of the user in the domain.
Effective Policy	Name of the profile assigned to the user in the domain.

Client Statistics

Charts	Information
Blocked Sites Distribution (past <number> days)	Displays the distribution of blocked sites in the past number of days. You can configure the number of days for which to display information. Go to *View* > *Settings* > *Log Settings*.
Top 10 Site Categories by Distribution (Past <number> Days)	Displays the distribution of top ten site categories in the past number of days. You can configure the number of days for which to display information. Go to *View* > *Settings* > *Log Settings*.

Blocked Sites (Past <number> Days)

Fields	Information
Time	Time the blocked site was visited.
Threat	Threat type detected.

Fields	Information
Client Version	Chromebook user's current version.
OS	Type of OS used by the Chromebook user.
URL	Blocked site's URL.
Port	Port number currently listening.
User Initiated	User initiated visitation to the blocked site.

Managing domains

You can manage domains from the *Google Domains* pane.

Editing domains

To edit domains:

1. Go to *Google Domains* > *Domains* and select a domain.
2. Click the *Edit* button.
3. Edit the options and click *Save Changes*.

Deleting domains

To delete domains:

1. Go to *Google Domains* > *Domains*, and select a domain.
2. Click the *Delete* button. A confirmation dialog displays.
3. Click *Yes*.

Endpoint Profiles

You can use the default endpoint profile or create endpoint profiles for many configurations and situations.

Configuring profiles

Profiles support web filtering by categories, black and white lists, and safe search. You can create different profiles and assign them to different groups in the Google domain.

Editing the default profile

You can edit the default profile to add or remove settings. You can revert to default settings by clicking *Revert to Default*.

To edit the default profile:

1. Go to *Endpoint Profiles*, and click the *Default* profile. The *Editing Profile: Default* pane displays.
2. Configure the settings on the tabs. See Profile references on page 54.
3. Click *Save Profile* to save the profile.

Adding new profiles

When you install FortiClient EMS for Chromebooks, a default profile is created. This profile is applied to any domains you add to FortiClient EMS for Chromebooks.

It is recommended to add Yandex search engine to the black list in the profile.

To create new profiles:

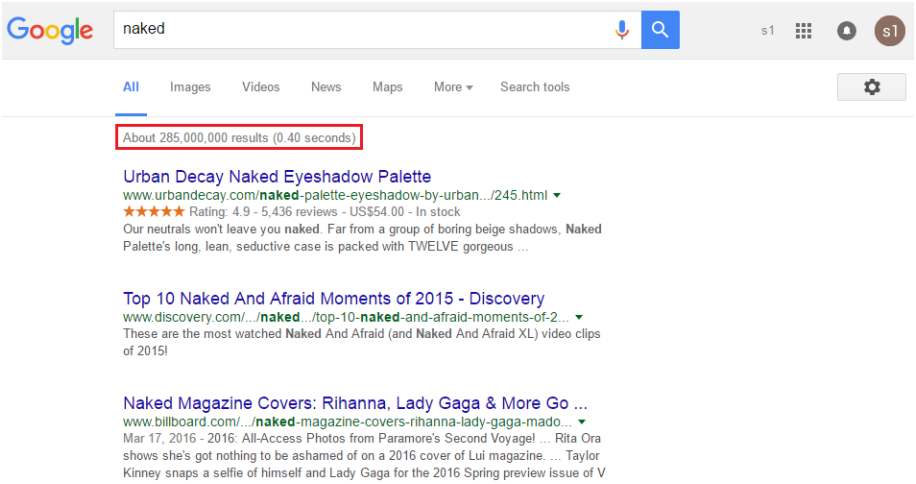
1. Go to *Endpoint Profiles* > *EMS Profiles*, and click *Add a new profile* button (the + button). The *Creating New Profile* pane displays.
2. In the *Profile Name* box, type the profile name.
3. On the *Web Filter* tab, enable *Web Filter*, and set the web filtering options.
4. On the *System Settings* tab, set the logging options.
5. Click *Save Profile* to save the profile.

Enabling/disabling Safe Search

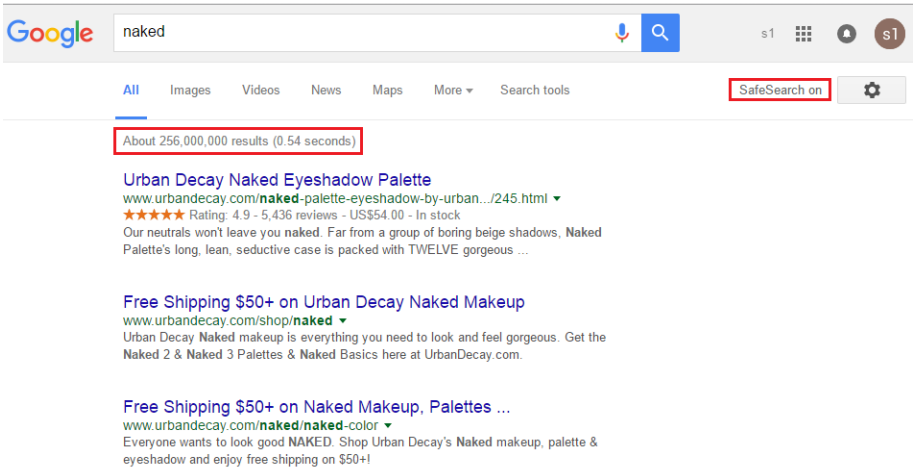
The search engine provides a Safe Search feature that blocks inappropriate or explicit images from search results. The Safe Search feature helps avoid most adult content. FortiClient EMS for Chromebooks supports Safe Search for most common search engines, such as Google, Yahoo, and Bing.

The profile in FortiClient EMS for Chromebooks controls the Safe Search feature.

Following are examples of search results with the Safe Search feature disabled and enabled. Notice the difference between the number of results. Here are the search results when the Safe Search feature is disabled, which has about 285000000 results:



Here are the search results when the Safe Search feature is enabled, which has about 256000000 results.



To enable or disable Safe Search:

1. In FortiClient EMS for Chromebooks, in the *Endpoint Profiles* area, click the *Default* profile or another profile.
2. On the *Web Filter* tab, enable or disable *Enable Safe Search*.

Viewing profiles

When you create endpoint profiles, they are listed under *Endpoint Profiles* in the left pane. You can view endpoint profiles and their settings.

To view profiles:

1. Go to *Endpoint Profiles*, and click *EMS Profiles*. The left pane displays the list of profiles.
2. Click a profile name. The settings display in the content pane.

Assigning profiles to Google Chromebooks

After creating the profile, you can assign the profile to Google domains. When you assign the profile to domains, the profile settings are automatically pushed to the Chromebooks in the domain.

To assign profiles:

1. Go to *Google Domains*.
2. Right-click a domain, select *Assign Profile*, then the profile. The profile is assigned.
3. Hover the mouse over the name of the domain to view the name of the assigned profile.

Managing profiles

You can manage profiles from the *Endpoint Profiles* pane.

Editing profiles

When you edit a profile assigned to domains, the changes are automatically pushed to the Chromebooks when you save the profile.

To edit profiles:

1. Go to *Endpoint Profiles*, and select a profile. The profile settings display in the content pane.
2. Edit the settings. See Profile references on page 54.
3. Click *Save Profile*. If the profile is assigned to domains, the changes are pushed to the domains.

Cloning profiles

To clone profiles:

1. Go to *Endpoint Profiles*.
2. Select a profile, and click the *Clone* button. The cloned profile displays in the content pane.
3. In the *Profile Name* box, type a name for the profile.
4. Configure the settings on the tabs. See Profile references on page 54.
5. Click *Save Profile*.

Deleting profiles

You cannot delete the default profile.

To delete profiles:

1. Go to *Endpoint Profiles*.
2. Click the *Delete* button beside the desired profile. A popup menu displays.
3. Click *Delete*. The profile is deleted.

Profile references

This section contains descriptions of the tabs and options used to configure profiles.

Web Filter

Configuration		Description
Web Filter		Enable or disable web filtering.
General		
	Log All URLs	Enable to log all URLs.
	Log User Initiated Traffic	Enable to log user initiated traffic.
	Enable Safe Search	Enable safe search. When safe search is enabled, the endpoint's Google search is set to *Restricted mode*, and YouTube access is set to *Strict Restricted access*. To set YouTube access to *Moderate Restricted* or *Unrestricted YouTube access*, you can disable Safe search and configure Google Search and YouTube access with the Google Admin Console instead of FortiClient EMS for Chromebooks.
Site Categories		
	Adult/Mature Content	Select one of the following: • Block • Warn • Allow • Monitor See the FortiGuard website for descriptions of the available categories and subcategories.

Configuration		Description
	Bandwidth Consuming	Select one of the following: • Block • Warn • Allow • Monitor See the FortiGuard website for descriptions of the available categories and subcategories.
	General Interest-Business	Select one of the following: • Block • Warn • Allow • Monitor See the FortiGuard website for descriptions of the available categories and subcategories.
	General Interest-Personal	Select one of the following: • Block • Warn • Allow • Monitor See the FortiGuard website for descriptions of the available categories and subcategories.
	Potentially Liable	Select one of the following: • Block • Warn • Allow • Monitor See the FortiGuard website for descriptions of the available categories and subcategories.
	Security Risk	Select one of the following: • Block • Warn • Allow • Monitor See the FortiGuard website for descriptions of the available categories and subcategories.

Configuration	Description
Unrated	Select one of the following: • Block • Warn • Allow • Monitor See the FortiGuard website for descriptions of the available categories and subcategories.
Exclusion List	
Action	Select one of the following actions: • Allow • Block • Monitor
URL	Enter specific URLs to allow, block, or monitor.
Type	Select one of the following types: • Simple • Wildcard • Regular Expression Wildcard characters and Perl Compatible Regular Expressions (PCRE) can be used.

System Settings

Configuration	Description
Log	Specify FortiClient log settings.
Level	Select one of the following: • Disabled • Emergency • Alert • Critical • Error • Warning • Notice • Info • Debug

Configuration		Description
Upload Logs to FortiAnalyzer/FortiManager		Turn on to upload FortiClient logs to the FortiAnalyzer or FortiManager device at the specified address or hostname.
	IP Address/Hostname	Enter the IP address. When connecting to FortiAnalyzer 5.6+, use the format *https://FAZ-IP:port/logging*. Otherwise, use the format *https://FAZ-IP/jsonrpc/fazapi/logs*.
	Upload Schedule (minutes)	Configure the upload schedule in minutes.
	Log Retention (days)	Configure the duration of time to retain logs in days.
	Compress Logs	Enable to compress logs.

User Management

This section describes the default user accounts and permissions for FortiClient EMS for Chromebooks. It also describes how to change the administrator password and configure Windows users.

Default user account and permissions

The default user named *admin* has complete access to all FortiClient EMS for Chromebooks permissions, including modification, user permissions, approval, discovery, and deployment.

Viewing users

You can view the default *admin* user and all users added to FortiClient EMS for Chromebooks.

To view users:

1. Go to *View* > *User Management*.
2. Click the *Administration* tab.
   The following information displays:

+Add	Add a new user.
Name	The username.
Access	Type of user access.
Type	Type of user.

Configuring User Management

Changing the admin password

By default, the *admin* user account has no password. You should add a password to increase security.

To change the admin password:

1. Go to *View* > *User Management*.
2. Select the *admin* account.
3. Click *Change Password* from the toolbar. Change your password.
4. Click *Save*.

Configuring Windows user accounts

You can configure Windows users to have no access or administrator access to FortiClient EMS for Chromebooks.

The Windows users list is derived from the server on which FortiClient EMS for Chromebooks is installed. If you want to add more Windows users, you must add them to the server.

To configure Windows users:

1. Go to *View* > *User Management*.
2. Click the *+Add* button from the toolbar.
3. Expand the *Add User* dropdown list.
4. Select the Windows user.
5. Perform one of the following actions:
   a. Select the specific domain access for the user. See Default user account and permissions on page 58.
   b. Configure the permissions.
6. Click *Save*.

Configuring Global Settings

To configure Global Settings:

1. Go to *View* > *User Management*.
2. Click *Global Settings*.
3. Set the following option:

Inactivity Timeout	Specify how long to keep inactive users logged into FortiClient EMS for Chromebooks. When the time expires, the user is automatically logged out of FortiClient EMS for Chromebooks. Type 0 to keep inactive users logged into FortiClient EMS for Chromebooks indefinitely.

4. Click *Save*.

User Management reference

This section contains descriptions of the fields used to configure User Management.

Windows users

Following is a description of the fields in *View* > *User Management* > *Add* > *User*.

Option		Description
Add User		Select the user to configure permissions for FortiClient EMS for Chromebooks.
Super Administrator permissions		Enable the super administrator feature to give the new Windows user super administrator permissions.
Comments		Enter optional comments/information for the Windows user.
Domain Access		Select or add access to a domain for the Windows user and configure their permissions. If you choose one or more domains in the domain access field, you must select specific permissions.
Permissions		Use the settings to configure permissions to FortiClient EMS for Chromebooks for the selected Windows user.
General		
	Create / Delete Filters	Select to allow the Windows user to create and delete filters. Clear to disable this permission.
Policies		
	Assign / Unassign Policy /	Select to allow the Windows user to assign to endpoints and unassign profiles from domains and manage custom groups. Clear to disable this permission.
	Create / Delete / Edit / Rename Policy	Select to allow the Windows user to create, delete, edit, and rename profiles. Clear to disable this permission.

View Menu

This section describes the options in the *View* menu.

License upgrades or renewals

Contact Fortinet Support to upgrade or renew your FortiClient EMS for Chromebooks license. After you have the license file, you can add it to FortiClient EMS for Chromebooks.

To upgrade or renew the FortiClient EMS for Chromebooks license:

1. Go to *View* > *Upgrade License*. The *Add FortiClient EMS License* pane displays.
2. Click *Browse*, and locate the license key file.
3. Click *Upload File*.

Database management

You can back up and restore the FortiClient EMS for Chromebooks database.

Backing up the database

To back up the database:

1. Go to *View* > *Database Management*. The *Database Backup/Restore* pane displays.
2. On the *Backup* tab, set the following options:

Password	Type a password for backing up and restoring the database.
Confirm Password	Retype the password to confirm it.

3. Click *Backup Database*.
   The database is backed up.

Restoring the database

To restore the database:

1. Go to *View* > *Database Management*. The *Database Backup/Restore* pane displays.
2. On the *Restore* tab, click *Browse*.
3. Locate the database backup file, and click *Open*.
4. In the *Password* box, type the password used to back up the database.

5. Click *Restore Database*.
   When the database is restored, a message appears. The message instructs you to wait for the restored database to reload.
6. Wait for the restored database to be reloaded.

Logs

You can view the log messages generated by FortiClient EMS for Chromebooks and download raw logs.

Viewing logs

To view log messages:

1. Go to *View* > *View Logs*. The *Logs* pane displays.
2. Click the *Filter* icon in each column heading to apply filters.
3. Click *Clear Filter* to remove the filters.

Downloading raw logs

You can download the raw logs generated by FortiClient EMS for Chromebooks.

To download raw logs:

1. Go to *View* > *View Logs*. The *Logs* pane displays.
2. Click *Raw Logs*.
3. Click the calendar icon in the *Start Date* and *End Date* boxes to select a start and end date for the logs to download.
4. From the *Levels* dropdown list, select one or more levels of logs to include.
5. From the *Sources* dropdown list, select one or more sources to include.
6. In the *Message* box, type the log message(s) to include. Leave blank to include all log messages.
   If you want to exclude the log message, enable the *NOT* option.
7. Click the *Calculate Size* button to view the size of the download.
8. Click *Download*.
   A zip of the raw logs is downloaded to your computer.

Settings

This section describes FortiClient EMS for Chromebooks settings.

Configuring Server Settings

FortiClient EMS for Chromebooks installs with a default IP address and port configured. You can change the IP address and port and configure other server settings for FortiClient EMS for Chromebooks.

To configure Server Settings:

1. Go to *View* > *Settings*.
2. Select *Server Settings*, and configure the following options:

Listen on IP Addresses	Displays the IP addresses for the FortiClient EMS for Chromebooks server. FortiClient registers to FortiClient EMS for Chromebooks on the specified IP address.
EMS has a FQDN	Turn on to specify a fully qualified domain name (FQDN) for the FortiClient EMS for Chromebooks server.
EMS FQDN	Displayed when *EMS has a FQDN* is turned on. Type the FQDN for the FortiClient EMS for Chromebooks server. FortiClient can register by using either the specified IP address in the *Listen on IP Addresses* option or the specified FQDN.
Remote Administration HTTPS Access	Specify settings for remote administration access to FortiClient EMS for Chromebooks. Turn remote HTTPS access to FortiClient EMS for Chromebooks console on and off. When enabled, type a host name in the *Custom Host Name* box to let administrators use a browser and HTTPS to log into the FortiClient EMS for Chromebooks console. When disabled, administrators can only log into FortiClient EMS for Chromebooks console on the server.
Pre-defined Host Name	Displays the pre-defined host name. The name cannot be changed.
Custom Host Name	Available when *Remote Administration HTTPS Access* is turned on. Displays the pre-defined host name of the server on which FortiClient EMS for Chromebooks is installed. You can customize the host name. When you change the host name, the web server restarts.
SSL Certificate	Displays the SSL certificate currently imported. If you have not imported an SSL certificate, a *No SSL certificate imported* message displays.
New SSL Certificate File	Upload a new SSL certificate.
New SSL Private Key	Upload a new SSL private key.
User Inactivity Timeout	Configure the user inactivity timeout in hours.

3. Click *Save*.

Configuring Log Settings

You can specify what level of log messages to capture in the logs for FortiClient EMS for Chromebooks. You can also specify when to automatically delete logs and alerts.

To configure Log Settings:

1. Go to *View* > *Settings*.
2. Under *Log Settings*, configure the following options:

Log Level	Select the level of messages to include in FortiClient EMS for Chromebooks logs. For example, if you select *Info*, all log messages from *Info* to *Emergency* are added to the FortiClient EMS for Chromebooks logs.
Auto Remove Logs	Type the number of days that you want to store logs. For example, if you type 30, logs will be stored for 30 days. Any logs older than 30 days are automatically deleted.
Remove All Logs	Click to immediately delete all FortiClient EMS for Chromebooks logs.
Auto Remove Web Filter Logs	Type the number of days that you want to keep violations. For example, if you type 30, violations will be kept for 30 days. Any violations older than 30 days are automatically deleted. The default is seven days.

3. Click *Save*.

Configuring the pre-login banner

When you enable the pre-login banner, a message appears prior to a user logging into EMS.

To enable and configure a pre-login banner:

1. Go to *View* > *Settings*.
2. Under *Pre-Login Banner*, enable *Enable Pre-login Banner*.
3. In the *Banner Message* box, type your message.
4. Click *Save*.

Configuring EMS for Chromebook

To configure Settings:

1. Go to *View* > *Settings*.
2. Click *EMS for Chromebook*, and configure the following options:

SSL Certificate	Displays the SSL certificate currently imported. If you have already uploaded an SSL certificate, a *Replace* button displays.

New SSL Certificate File	Browse and upload a new SSL certificate file. See Adding SSL certificates to FortiClient EMS for Chromebooks on page 65.
New SSL Password	Configure a new SSL password.
Listen on Port	Displays the default port for the FortiClient EMS for Chromebooks server. You can change the port by typing a new port number. FortiClient connects to FortiClient EMS for Chromebooks using the specified port number.
Profile Update Interval	Specify the profile update interval (in seconds).
Service Account ID	Displays the service account ID currently in use.
Reset	In the event your service account is broken, you can revert back to the default service account by clicking the *Reset* button. This restores the default service account. You need to *Save* the settings for the change to take effect.
New Service Account ID	Enter a new service account ID.
New Service Account Private Key	Enter a new service account private key.

3. Click *Save*.

Adding SSL certificates to FortiClient EMS for Chromebooks

You must add an SSL certificate to FortiClient EMS for Chromebooks to allow HTTPS connections with the Google Admin console.

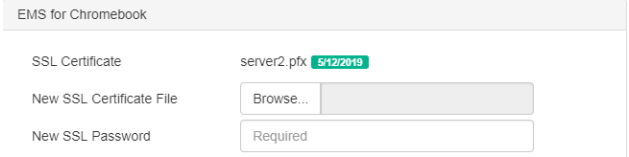
If you are using a public SSL certificate, add the certificate to FortiClient EMS for Chromebooks. You do not need to add the certificate to the Google Admin console.

If you are not using a public SSL certificate, you must add the SSL certificate to FortiClient EMS for Chromebooks, and the root certificate to the Google Admin console. See Adding root certificates on page 30.

To add or replace SSL certificates:

1. In FortiClient EMS for Chromebooks, go to *View* > *Settings*.
2. Click the *EMS for Chromebook* tab.
3. Beside *New SSL Certificate File*, click *Browse*, and locate the certificate file (<name>.pfx).
4. In the *New SSL Password* box, type the password.
5. Click *Test*.
6. Click *Save*.

If the SSL certificate is expiring in less than three months, the expiry date label is yellow; if it has expired, the label is red. Otherwise, it is green.



Configuring email alert settings

You can set up an SMTP server to enable alerts for EMS events. When an alert is triggered, an email notification is sent.

To configure email alerts and an SMTP server:

1. Go to *View* > *Settings* > *E-mail Alerts*.
2. Enable *Send E-Mail Alerts for the Following EMS Events*, and set the following options:

Notify when new EMS versions are available for deployment		New EMS versions are available.
	Remind me everyday for 2 weeks	Enable to remind you when new EMS versions are available everyday for two weeks.
Notify when EMS license is expiring or expired		Expiring or expired EMS license.

3. Click *Save*.
   If you have not already set up an SMTP server, the GUI automatically prompts you to configure *SMTP Server Settings*. See Configuring SMTP Server Settings on page 66.

Configuring SMTP Server Settings

You can set up an SMTP server to enable alerts for EMS events. When an alert is triggered, an email notification is sent.

To configure SMTP Server Settings:

1. Go to *View* > *Settings* > *E-mail Alerts*, and enable *Send E-Mail Alerts for the Following EMS Events*.
   The *SMTP Server Settings* option displays under *Alerts*.
2. Click *SMTP Server Settings*, and set the following options:

SMTP Server		Enter the SMTP server.
Port		Enter the port number.
Security		Select *None*, *STARTTLS*, or *SMTPS* for the security type, or select the *Auto Detect* button to automatically select the security type. If *STARTTLS* or *SMTPS* is selected, the *Username* and *Password* boxes become available.
	Username	Enter the username.
	Password	Enter the password.

From Address	Enter the email address to send the alerts from.
Reply To	Enter the email address to send the replies to.
Subject	The sent e-mail alert's subject.
Recipients	Enter email address(es) to send alerts to. Click the + button to add more email addresses.
Test Email Settings	Click the button to test the configured email settings.

3. Click *Save*.

Creating a support package

You can create a support package to provide to the Fortinet technical support team for troubleshooting. Creating a support package backs up your database, but clears all sensitive username and password fields.

To create a support package:

1. Go to *Help* > *Create Support Package*. The *Create Support Package* dialog box displays.
2. In the *Password* box, type your administrative password.
3. In the *Confirm Password* box, type your password again.
4. Click *Create Support Package*.